MODELS OF $\mathbb{Z}/p^2\mathbb{Z}$ OVER A D.V.R. OF UNEQUAL CHARACTERISTIC

DAJANO TOSSICI

Abstract. Let R be a discrete valuation ring of unequal characteristic which contains a primitive p^2-th root of unity. If K is the fraction field of R, it is well known that $(\mathbb{Z}/p^2\mathbb{Z})_K \simeq \mu_{p^2,K}$. We prove that any finite and flat R-group scheme of order p^2 isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})_K$ on the generic fiber (i.e. a model of $(\mathbb{Z}/p^2\mathbb{Z})_K$), is the kernel in a short exact sequence which generically coincides with the Kummer sequence. We will explicitly describe and classify such models.

Contents

Introduction

Notation and Conventions. If not otherwise specified we denote by R a discrete valuation ring (in the sequel d.v.r.) of unequal characteristic, i.e. a d.v.r. with fraction field K of characteristic zero and with residue field k of characteristic $p > 0$. Moreover we write $S = \mathrm{Spec}(R)$. If, for $n \in \mathbb{N}$, there exists a distinguished primitive p^n-th root of unity ζ_n in a d.v.r. R, we call $\lambda_{(n)} := \zeta_n - 1$. We remark that $v(\lambda_{(n-1)}) = pv(\lambda_{(n)})$ and $v(p) = p^{n-1}(p-1)v(\lambda_n)$. Moreover, for any $i \leq n$, we suppose $\zeta_{i-1} = \zeta_i^p$. And we will denote by $\pi \in R$ one of its uniformizers. Moreover if G is an affine R-group scheme we will denote by $R[G]$ the associated Hopf algebra. All the schemes will be assumed noœtherian.

Let K be a field of characteristic 0 which contains a primitive p^n-th root of unity. We remark that this implies $\mu_{p^n} \simeq \mathbb{Z}/p^n\mathbb{Z}$. We recall the following exact sequence

$$1 \longrightarrow \mu_{p^n} \longrightarrow \mathbb{G}_m \xrightarrow{p^n} \mathbb{G}_m \longrightarrow 1,$$

so-called the Kummer sequence. The Kummer theory says that any p^n-cyclic Galois extension of K can be deduced by the Kummer sequence. We stress that the Kummer sequence can be written also as follows

$$1 \longrightarrow \mu_{p^n} \longrightarrow \mathbb{G}_m^n \xrightarrow{\theta_n} \mathbb{G}_m^n \longrightarrow 1$$

where $\theta_n((T_1,\dots,T_n)) = (1-T_1^p, T_1 - T_2^p, \dots, T_{n-1} - T_n^p)$.

Let k be a field of characteristic $p>0$. The following exact sequence

$$0 \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow W_n(k) \xrightarrow{\mathrm{F}-1} W_n(k) \longrightarrow 0,$$

where $W_n(k)$ is the group scheme of Witt vectors of length n, is called the Artin-Schreier-Witt sequence. The Artin-Schreier-Witt theory implies that any p^n-cyclic Galois covering of k can be deduced by the Artin-Schreier-Witt sequence.

Let now R be a d.v.r. of unequal characteristic which contains a p^n-th root of unity. It has been proved, independently, by Oort-Sekiguchi-Suwa ([14]) and Waterhouse ([27]) the existence of an exact sequence of group schemes over R which unifies the above two sequences for $n=1$. Later Green-Matignon ([5]) and Sekiguchi-Suwa([22]) have, independently, constructed explicitly a unifying exact sequence for $n=2$. This means that it has been found an exact sequence

$$0 \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathcal{W}_2 \longrightarrow \mathcal{W}'_2 \longrightarrow 0 \tag{1}$$

that coincides with the Kummer sequence on the generic fiber and with the Artin-Schreier-Witt sequence on the special fiber. The case $n>2$ is treated in [13] and [21]. In this paper we focus on finite and flat R-group schemes of order p^2 which are isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})_K$ on the generic fiber, i.e. models of $(\mathbb{Z}/p^2\mathbb{Z})_K$. And we will prove that, for any such a group scheme G, there exists an exact sequence

$$0 \longrightarrow G \longrightarrow \mathcal{E}_1 \longrightarrow \mathcal{E}_2 \longrightarrow 0,$$

with $\mathcal{E}_1, \mathcal{E}_2$ smooth R-group schemes, which coincides with the Kummer sequence on the generic fiber. We will describe explicitly all such isogenies and their kernels. Moreover we will give a classification of models of $(\mathbb{Z}/p^2\mathbb{Z})_K$.

We now explain more precisely the classification we have obtained. The first two sections are devoted to review some known facts: in the first one we recall the definition of a class of group schemes of order p^n, called $G_{\lambda,n}$, which are isomorphic to μ_{p^n} on the generic fiber; in the second one we recall some results about Neron blow-ups.

In the third section we recall the following well known result about classification of models of $(\mathbb{Z}/p\mathbb{Z})_K$.

Theorem. *3.1. Let suppose that R contain a primitive p-th root of unity. If G is a finite and flat R-group scheme such that $G_K \simeq (\mathbb{Z}/p\mathbb{Z})_K$ then $G \simeq G_{\lambda,1}$ for some $\lambda \in R$.*

In §4 we study the models of $(\mathbb{Z}/p^2\mathbb{Z})_K$. Let us suppose that R contains a primitive p^2-th root of unity. We remark that this hypothesis is only used to conclude that $(\mathbb{Z}/p^2\mathbb{Z})_K \simeq (\mu_{p^2})_K$. Without this hypothesis what follows remains true substituting $(\mathbb{Z}/p^2\mathbb{Z})_K$ with $(\mu_{p^2})_K$. First of all we show that any model of $(\mathbb{Z}/p^2\mathbb{Z})_K$ is an extension of $G_{\mu,1}$ by $G_{\lambda,1}$ for some $\mu,\lambda \in R\setminus\{0\}$. So we reduce ourselves to investigate on $\mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$.

Let $S_\lambda := \mathrm{Spec}(R/\lambda R)$ and let us define the group

$$rad_{p,\lambda}(<1+\mu S>) := \Big\{ (F(S), j) \in \mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}}, \mathbb{G}_{m|S_\lambda}) \times \mathbb{Z}/p\mathbb{Z} \text{ such that }$$
$$F(S)^p(1+\mu S)^{-j} = 1 \in \mathrm{Hom}(G_{\mu,1_{|S_{\lambda^p}}}, \mathbb{G}_{m|S_{\lambda^p}}) \Big\} / <1+\mu S> .$$

There is an abuse of notation since S denotes both $\mathrm{Spec}(R)$ and the indeterminate of some polynomials. For any $(F,j) \in rad_{p,\lambda}(< 1+\mu S >)$ we will explicitly define in 4.4 an extension $\mathcal{E}^{(\mu,\lambda;F,j)}$ of $G_{\mu,1}$ by $G_{\lambda,1}$. As a group scheme $\mathcal{E}^{(\mu,\lambda;F,j)}$ is the kernel of an isogeny of smooth group schemes of dimension 2. This isogeny generically is isomorphic to the morphism θ_n defined above. Using this notation, we will give a description of $\mathrm{Ext}^1(G_{\mu,1},G_{\lambda,1})$.

Theorem. *4.39. Suppose that $\lambda,\mu \in R$ with $v(\lambda_{(1)}) \geq v(\lambda), v(\mu)$. There exists an exact sequence*

$$0 \longrightarrow rad_{p,\lambda}(< 1+\mu S >) \xrightarrow{\beta} \mathrm{Ext}^1(G_{\mu,1},G_{\lambda,1}) \longrightarrow$$
$$\longrightarrow \ker\left(H^1(S,G^\vee_{\mu,1}) \longrightarrow H^1(S_\lambda,G^\vee_{\mu,1})\right)$$

where β is defined by

$$(F,j) \longmapsto \mathcal{E}^{(\mu,\lambda;F,j)}.$$

In particular the set $\{\mathcal{E}^{(\mu,\lambda;F,j)}\} \subseteq \mathrm{Ext}^1(G_{\mu,1},G_{\lambda,1})$ is a group isomorphic to $rad_{p,\lambda}(< 1+\mu S >)$.

The group $\mathrm{Ext}^1(G_{\mu,1},G_{\lambda,1})$ has been described by Greither in [6] through a short exact sequence, different by that of the previous theorem. An advantage of our description is that we individuate a class of extensions which, if we forget the structure of extension, "essentially" covers all the group schemes of order p^2. Indeed from 4.39 it follows that any group scheme of order p^2, up to an extension of R, is of the form $\mathcal{E}^{(\mu,\lambda;F,j)}$ (see 4.43). Using the Sekiguchi-Suwa theory, which is briefly explained in §4.2, we obtain the following result.

Corollary. *4.47 Let us suppose $p > 2$. Let $\mu,\lambda \in R\setminus\{0\}$ be with $v(\lambda_{(1)}) \geq v(\mu) \geq v(\lambda)$. Then, the group $\{\mathcal{E}^{(\mu,\lambda;F,j)}\}$ is isomorphic to the group*

$$\Phi_{\mu,\lambda} := \left\{(a,j) \in (R/\lambda R)\times \mathbb{Z}/p\mathbb{Z} \text{ such that } a^p = 0 \text{ and } pa - j\mu = \frac{p}{\mu^{p-1}}a^p \in R/\lambda^p R\right\},$$

through the map

$$(a,j) \longmapsto \mathcal{E}^{(\mu,\lambda;\sum_{i=0}^{p-1}\frac{a^i}{i!}S^i,j)}.$$

We give also a similar description of the group $\{\mathcal{E}^{(\mu,\lambda;F,j)}\}$ with $v(\mu) < v(\lambda)$: see 4.45. Moreover we remark that we can explicitly find all the solutions a of the equation $pa - j\mu \equiv \frac{p}{\mu^{(p-1)}}a^p \mod \lambda^p$ if $v(\mu) \geq v(\lambda)$(see 4.51).

In §5 we are interested in the group schemes which are models of $(\mathbb{Z}/p^2\mathbb{Z})_K$. We prove the following theorem.

Theorem. *4.58 Let us suppose $p > 2$. Let G be a finite and flat R-group scheme such that $G_K \simeq (\mathbb{Z}/p^2\mathbb{Z})_K$. Then $G \simeq \mathcal{E}^{(\pi^m,\pi^n;\sum_{i=0}^{p-1}\frac{a^i}{i!}S^i,1)}$ for some $v(\lambda_{(1)}) \geq m \geq n \geq 0$ and $(a,1) \in \Phi_{\pi^m,\pi^n}$. Moreover m,n and $a \in R/\pi^n R$ are unique.*

The last section is devoted to determine, through the description of 4.47, the special fibers of the extensions which, as group schemes, are models of $(\mathbb{Z}/p^2\mathbb{Z})_K$.

The explicit description of the models of $(\mathbb{Z}/p^2\mathbb{Z})_K$ presented in this paper will be used in [24] to study the degeneration of $\mathbb{Z}/p^2\mathbb{Z}$-torsors from characteristic 0 to characteristic p.

Acknowledgments This paper constitutes part of my PhD thesis. It is a pleasure to thank Professor Carlo Gasbarri for his guidance and his constant encouragement. I begun this work during my visit to Professor Michel Matignon in 2005 at the Department of Mathematics of the University of Bordeaux 1. I am indebted to him for the useful conversations and for his great interest in my work. I am deeply grateful to Matthieu Romagny for his very careful reading of this paper and for his several comments, suggestions, remarks and answers to my questions. I wish also to thank Professor Fabrizio Andreatta for having suggested me the sketch of proof of 4.27. Finally I thank Filippo Viviani for the stimulating and useful conversations.

1. Some group schemes of order p^n

For any $\lambda \in R$ define the group scheme

$$\mathcal{G}^{(\lambda)} = \mathrm{Spec}(R[T, \frac{1}{1+\lambda T}])$$

The R-group scheme structure is given by

$$\begin{aligned} &T \longrightarrow 1 \otimes T + T \otimes 1 + \lambda T \otimes T && \text{comultiplication} \\ &T \longrightarrow 0 && \text{counit} \\ &T \longrightarrow -\frac{T}{1+\lambda T} && \text{coinverse} \end{aligned}$$

We observe that if $\lambda = 0$ then $\mathcal{G}^{(\lambda)} \simeq \mathbb{G}_a$. It is possible to prove that $\mathcal{G}^{(\lambda)} \simeq \mathcal{G}^{(\mu)}$ if and only if $v(\lambda) = v(\mu)$ and the isomorphism is given by $T \longrightarrow \frac{\lambda}{\mu} T$. Moreover it is easy to see that, if $\lambda \in \pi R \setminus \{0\}$, then $\mathcal{G}_k^{(\lambda)} \simeq \mathbb{G}_a$ and $\mathcal{G}_K^{(\lambda)} \simeq \mathbb{G}_m$. It has been proved by Waterhouse and Weisfeiler, in [28, 2.5], that any deformation, as a group scheme, of $\mathbb{G}_a$ to $\mathbb{G}_m$ is isomorphic to $\mathcal{G}^{(\lambda)}$ for some $\lambda \in \pi R \setminus \{0\}$. If $\lambda \in R \setminus \{0\}$ we can define the morphism

$$\alpha^\lambda : \mathcal{G}^{(\lambda)} \longrightarrow \mathbb{G}_m$$

given, on the level of Hopf algebras, by $x \longmapsto 1 + \lambda x$: it is an isomorphism on the generic fiber. If $v(\lambda) = 0$ then α^λ is an isomorphism.

We now define some finite and flat group schemes of order p^n. Let $\lambda \in R$ satisfy the condition

$$(*) \qquad v(p) \geq p^{n-1}(p-1)v(\lambda).$$

Then the map

$$\begin{aligned} \psi_{\lambda,n} : &\mathcal{G}^{(\lambda)} \longrightarrow \mathcal{G}^{(\lambda^{p^n})} \\ &T \longrightarrow P_{\lambda,n}(T) := \frac{(1+\lambda T)^{p^n} - 1}{\lambda^{p^n}} \end{aligned}$$

is an isogeny of degree p^n. Let

$$G_{\lambda,n} := \mathrm{Spec}(R[T]/P_{\lambda,n}(T))$$

be its kernel. It is a commutative finite flat group scheme over R of rank p^n. It is possible to prove that

$$\begin{aligned} (G_{\lambda,n})_k &\simeq \mu_{p^n} && \text{if } v(\lambda) = 0 \\ (G_{\lambda,n})_k &\simeq \alpha_{p^n} && \text{if } p^{n-1}(p-1)v(\lambda) < v(p); \\ (G_{\lambda,n})_k &\simeq \alpha_{p^{n-1}} \times \mathbb{Z}/p\mathbb{Z} && \text{if } p^{n-1}(p-1)v(\lambda) = v(p). \end{aligned}$$

We observe that α^λ is compatible with $\psi_{\lambda,n}$, i.e the following diagram is commutative

$$(2) \qquad \begin{tikzcd} \mathcal{G}^{(\lambda)} \arrow[r, "\alpha^\lambda"] \arrow[d, "\psi_{\lambda,n}"'] & \mathbb{G}_m \arrow[d, "p^n"] \\ \mathcal{G}^{(\lambda^{p^n})} \arrow[r, "\alpha^{\lambda^{p^n}}"] & \mathbb{G}_m \end{tikzcd}$$

Then it induces a map

$$\alpha^{\lambda,n} : G_{\lambda,n} \longrightarrow \mu_{p^n}$$

which is an isomorphism on the generic fiber. And if $v(\lambda) = 0$ then $\alpha^{\lambda,n}$ is an isomorphism.

We remark that

$$\mathrm{Hom}(G_{\lambda,n}, G_{\lambda',n}) = \begin{cases} 0, & \text{if } v(\lambda) < v(\lambda'); \\ \mathbb{Z}/p^n\mathbb{Z}, & \text{otherwise.} \end{cases}$$

If $v(\lambda) \geq v(\lambda')$ the morphisms are given by

$$\begin{aligned} G_{\lambda,n} &\longrightarrow G_{\lambda',n} \\ T &\longmapsto \frac{(1+\lambda T)^i - 1}{\lambda'} \end{aligned}$$

for $i = 0, \ldots, p^n - 1$. It follows easily that $G_{\lambda,n} \simeq G_{\lambda',n}$ if and only if $v(\lambda) = v(\lambda')$.

In the following any time we will speak about $G_{\lambda,n}$ it will be assumed that λ satisfies $(*)$. If R contains a primitive p^n-th root of unity ζ_n then, since

$$v(p) = p^{n-1}(p-1)v(\lambda_{(n)}),$$

the condition $(*)$ is equivalent to $v(\lambda) \leq v(\lambda_{(n)})$.

2. Néron blow-ups

We recall here the definition of Néron blow-up. For details see [3, Ch. 3], [16] and [28]. In this section R is a not necessarily of unequal characteristic.

Definition 2.1. Let X be a flat affine R-scheme of finite type and $R[X]$ its coordinate ring. Let Y be a closed subscheme of X_k defined by some proper ideal $I(Y)$ of $R[X]$. Then $\pi \in I(Y)$. We define the *Néron blow-up* (or *dilatation*) of Y in X by

$$X^Y := \operatorname{Spec}(A[\pi^{-1}I(Y)]).$$

Then X^Y is a flat affine R-scheme of finite type and the R-homomorphism $R[X] \subseteq R[\pi^{-1}I(Y)]$ induces a morphism

$$X^Y \longrightarrow X,$$

which gives an isomorphism on the generic fiber.

The Néron-blow up is explicitly given as follows: let $I = (\pi, f_1, \ldots, f_k)$ with $f_i \in R$. Then

$$R[X^Y] = R[X][\pi^{-1}f_1, \ldots, \pi^{-1}f_k].$$

So X^Y is the open set of $x \in \operatorname{Proj}(\oplus_{i\geq 0} I^i)$ (the classical blow-up of X in Y), where I_x is generated by π. Clearly it is possible to give the definition for schemes in general (see [3, Ch. 3]).

In the following we are interested in the case where X is an affine flat group scheme G and Y a subgroupscheme H of G_k. We recall the following definitions.

Definition 2.2. Let $\varphi : G \longrightarrow H$ be a morphism of flat R-group schemes which is an isomorphism restricted to the generic fibers. Then it is called a *model map*.

Definition 2.3. Let H_K be a group scheme over K. Any flat R-group scheme G such that $G_K \simeq H_K$ is called a *model* of H_K.

It is possible to prove that G^H is a group scheme and $G^H \longrightarrow G$ is a model map ([28, 1.1]). We recall the following results:

Proposition 2.4. *The canonical map $G^H \longrightarrow G$ sends the special fiber into H. Moreover G^H has the following universal property: any model map $G' \longrightarrow G$ sending the special fiber into H factors uniquely through G^H.*

Proof. [28, 1.2]. □

Theorem 2.5. *Any model map between affine group schemes is isomorphic to a composite of Néron blow-ups.*

Proof. [28, 1.4]. □

Example 2.6. Let us consider the group scheme $G_{\mu,1} = \mathrm{Spec}(R[S]/(\frac{(1+\mu S)^p-1}{\mu^p}))$ with $v(p) > (p-1)v(\mu)$. The only possible subgroup of $(G_{\mu,1})_k$ which gives a nontrivial blow-up is $H = e$. Then $I(H) = (\pi, S)$ if $v(\mu) > 0$ and $I(H) = (\pi, S-1)$ otherwise. It is easy to see that, in both cases,

$$G^e_{\mu,1} = G_{\mu\pi,1}.$$

So if there exists a model map $G \longrightarrow G_{\mu,1}$ then, using 2.5, $G \simeq G_{\lambda,1}$ for some $\lambda \in R$.

3. Models of $(\mathbb{Z}/p\mathbb{Z})_K$

We now recall the classification of $(\mathbb{Z}/p\mathbb{Z})_K$-models. Two proofs of this result are for instance given in [12, 1.4.4, 3.2.2]. The second one is essentially that we present here. We remark that if G is a model of $(\mathbb{Z}/m\mathbb{Z})_K$ and R contains a primitive m-th root of unity then there are the following model maps

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow G \longrightarrow \mu_m.$$

Indeed the first one is the normalization map, while the second one is the dual morphism of the normalization $\mathbb{Z}/m\mathbb{Z} \longrightarrow G^\vee$ (see also [10, 2.2.3] for a more general result).

Proposition 3.1. *Let us suppose that R contains a primitive p-th root of unity. If G is a finite and flat R-group scheme such that $G_K \simeq \mathbb{Z}/p\mathbb{Z}$ then $G \simeq G_{\lambda,1}$ for some $\lambda \in R \setminus \{0\}$.*

Proof. As remarked above we have an R-model map

$$\varphi : G \longrightarrow \mu_p.$$

By 2.5 it is a composition of Néron blow-ups. Then, by 2.6, it follows that $G \simeq G_{\lambda,1}$ for some $\lambda \in R \setminus \{0\}$. □

4. Models of $(\mathbb{Z}/p^2\mathbb{Z})_K$

In this section we study models of $(\mathbb{Z}/p^2\mathbb{Z})_K$. Throughout the section we suppose that R contains a primitive p^2-th root of unity. First of all we prove that any such group is an extension of $G_{\mu,1}$ by $G_{\lambda,1}$ for some $\mu, \lambda \in R \setminus \{0\}$.

Lemma 4.1. *Let G be a finite and flat R-group scheme of order p^2 such that G_K is a constant group. Then G is an extension of $G_{\mu,1}$ by $G_{\lambda,1}$ for some $\mu, \lambda \in R \setminus \{0\}$.*

Proof. If G_K is a constant group then G_K is isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})_K$ or to $(\mathbb{Z}/p\mathbb{Z})_K \times (\mathbb{Z}/p\mathbb{Z})_K$. We consider the factorization

$$0 \longrightarrow (\mathbb{Z}/p\mathbb{Z})_K \longrightarrow G_K \longrightarrow (\mathbb{Z}/p\mathbb{Z})_K \longrightarrow 0.$$

We take the closure G_1 of $(\mathbb{Z}/p\mathbb{Z})_K$ in G. Then G_1 is a model of $(\mathbb{Z}/p\mathbb{Z})_K$. So by 3.1 it follows that $G_1 \simeq G_{\lambda,1}$ for some $\lambda \in R \setminus \{0\}$. $G/G_{\lambda,1}$ is a model of $(\mathbb{Z}/p\mathbb{Z})_K$, too. So, again by 3.1, we have $G/G_{\lambda,1} \simeq G_{\mu,1}$ for some $\mu \in R \setminus \{0\}$. We are done. □

So we study, first of all, the group $\mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$.

4.1. Extensions of group schemes.

We here recall some generalities on extensions of group schemes. For more details see [4, III.6].

Let G and H be group schemes on S. We moreover suppose that H is commutative and that G acts on H. Let us denote

$$\mathrm{Ext}^0_S(G,H) = \{\varphi \in \mathrm{Hom}_{Sch_S}(G,H) | \varphi(gg') = \varphi(g) + g(\varphi(g')) \text{ for any local sections } g, g' \text{ of } G\}.$$

We are interested in the case that G acts trivially on H. In this situation

$$\mathrm{Ext}^0_S(G,H) = \mathrm{Hom}_{gr}(G,H).$$

Now $H \mapsto \mathrm{Ext}^0(G,H)$ is a left exact functor from the category of fppf-sheaves of G-modules on S to that of abelian groups. Let $\mathrm{Ext}^\bullet_S(G,H)$ denote the left derived functor of $H \mapsto \mathrm{Ext}^0_S(G,H)$. It is known that $\mathrm{Ext}^1_S(G,H)$ is isomorphic to the group of equivalence classes of extensions of G by H (see [4, III 6.2]).

Recall that an extension of G by H is by definition an exact sequence of fppf-sheaves of groups

$$0 \longrightarrow H \xrightarrow{i} E \xrightarrow{j} G \longrightarrow 0,$$

such that $i(j(g)h) = gi(h)g^{-1}$ for any local sections h of H and g of E.

Consider two extensions $(E) : 0 \longrightarrow H \xrightarrow{i} E \xrightarrow{j} G \longrightarrow 0$ and $(F) : 0 \longrightarrow H \xrightarrow{i} F \xrightarrow{j} G \longrightarrow 0$. They are equivalent if there exists a morphism of group schemes $f : E \longrightarrow F$ which makes the following diagram

$$\begin{tikzcd}
(E) : 0 \arrow[r] & H \arrow[r, "i"] \arrow[d, equal] & E \arrow[r, "j"] \arrow[d, "f"] & G \arrow[r] \arrow[d, equal] & 0 \\
(F) : 0 \arrow[r] & H \arrow[r, "i"] & F \arrow[r, "j"] & G \arrow[r] & 0
\end{tikzcd}$$

commute. Clearly such an f is an isomorphism of group schemes. If G and H are flat affine groups over S, then it is the same for E.

We now recall the definitions of pushforward and pull-back of extensions. Let G and H be as above and $\varphi : G' \longrightarrow G$ a morphism of group-schemes. Then φ induces a morphism

$$\varphi^* : \mathrm{Ext}^1_S(G,H) \longrightarrow \mathrm{Ext}^1_S(G',H).$$

It is explicitly given as follows. Let

$$(E) : 0 \longrightarrow H \xrightarrow{i} E \xrightarrow{j} G \longrightarrow 0$$

be an extension of G by H. Then $\varphi^*[E]$ is defined by the diagram

$$\begin{tikzcd}
\varphi^*[E] : 0 \arrow[r] & H \arrow[r, "i"] \arrow[d, equal] & E' \arrow[r, "j"] \arrow[d] & G' \arrow[r] \arrow[d, "\varphi"] & 0 \\
(E) : 0 \arrow[r] & H \arrow[r, "i"] & E' \arrow[r, "j"] & G \arrow[r] & 0
\end{tikzcd}$$

where the right square is cartesian.

Now consider a group scheme H' together with a G-action. If $\psi : H \longrightarrow H'$ is a morphism which preserves the G-action then it induces a morphism

$$\psi_* : \mathrm{Ext}^1_S(G,H) \longrightarrow \mathrm{Ext}^1_S(G,H'),$$

which we can explicitly describe as follows. Let

$$(E) : 0 \longrightarrow H \xrightarrow{i} E \xrightarrow{j} G \longrightarrow 0$$

be an extension of G by H. Then $\psi_*[E]$ is defined by the diagram

$$\begin{tikzcd}
(E) : 0 \arrow[r] & H \arrow[r, "i"] \arrow[d, "\psi"] & E \arrow[r, "j"] \arrow[d] & G \arrow[r] \arrow[d, equal] & 0 \\
\psi_*[E] : 0 \arrow[r] & H' \arrow[r, "i"] & E' \arrow[r, "j"] & G \arrow[r] & 0
\end{tikzcd}$$

where the left square is cocartesian.

Next we recall the Hochschild cohomology. Let G be a presheaf of groups on $Sch_{|S}$ and F a presheaf of G-modules on $Sch_{|S}$. We define a complex $\{C^n(G,F), \delta^n\}$ as follows: $C^n(G,F)$ denotes the set of morphisms of schemes from G^n to H and the boundary map

$$\delta^n : C^n(G,F) \longrightarrow C^{n+1}(G,F)$$

is defined by

$$(\delta^n f)(g_0, g_1, \dots, g_n) = g_0 f(g_1, \dots, g_n) + \\ + \sum_{i=0}^{n-1} (-1)^{i+1} f(g_0, g_1, \dots, g_i g_{i+1}, \quad \dots, g_n) + (-1)^{n+2} f(g_0, g_1, \dots, g_{n-1}).$$

Put

$$Z^n(G,F) = \ker(\delta^n : C^n(G,F) \longrightarrow C^{n+1}(G,F)),$$
$$B^n(G,F) = Im(\delta^{n-1} : C^{n-1}(G,F) \longrightarrow C^n(G,F)),$$

and

$$H_0^n(G,F) = Z^n(F,G)/B^n(G,F).$$

For our purposes we are interested in the second group of cohomology. The following result is indeed well known.

Proposition 4.2. *Let G and H be group schemes over S. Given an action of G on H then $H_0^2(G,H)$ is isomorphic to the group of equivalence classes of extensions of G by H which have a scheme-theoretic section.*

Proof. [4]. □

4.2. **Sekiguchi-Suwa Theory.** Here is a very partial review of results of [16], [18] and [22]. Let $\mu, \lambda \in \pi R \setminus \{0\}$. For any $\lambda' \in R \setminus \{0\}$ set $S_{\lambda'} = \mathrm{Spec}(R/\lambda' R)$. What we call Sekiguchi-Suwa theory is their description of $\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$ and $\mathrm{Ext}^1(\mathcal{G}^{(\mu)}, \mathcal{G}^{(\lambda)})$ through Witt vectors.

Let $Y = \mathrm{Spec}(R[T_1, \dots, T_m]/(F_1, \dots, F_n))$ be an affine R-scheme of finite type. We recall that, for any R-scheme X we have that $\mathrm{Hom}_{Sch}(X,Y)$ is in bijective correspondence with the set

$$\{(a_1, \dots, a_m) \in H^0(Y, \mathcal{O}_Y)^m | F_1(a_1, \dots, a_m) = 0, \dots, F_n(a_1, \dots, a_m) = 0\}.$$

With an abuse of notation we will identify these two sets. If X and Y are R-group schemes we will also identify $\mathrm{Hom}_{gr}(X,Y)$ with a subset of

$$\{(a_1, \dots, a_m) \in H^0(Y, \mathcal{O}_Y)^m | F_1(a_1, \dots, a_m) = 0, \dots, F_n(a_1, \dots, a_m) = 0\}.$$

We now fix presentations for the group schemes $\mathbb{G}_m$ and $\mathcal{G}^{(\lambda)}$ with $\lambda \in \pi R$. Indeed we write $\mathbb{G}_m = \mathrm{Spec}(R[S, 1/S])$ and $\mathcal{G}^{(\lambda)} = \mathrm{Spec}(R[S, 1/1 + \lambda S])$. We remark again that throughout the paper will be a conflict of notation since S will denote both $\mathrm{Spec}(R)$ and an indeterminate. But it should not cause any problem. Before illustrating the Sekiguchi-Suwa theory we see what happens when $\mu \in R^*$. In this case $\mathcal{G}^{(\mu)} \simeq \mathbb{G}_m$, and we have the following well known lemma.

Lemma 4.3. *For any $\lambda \in \pi R$ we have*

$$\mathrm{Hom}_{gr}(\mathbb{G}_{m|S_\lambda}, \mathbb{G}_{m|S_\lambda}) = \{S^i \in R[S, 1/S] | i \in \mathbb{Z}\}.$$

In particular if $v(\lambda_1) \geq v(\lambda_2) > 0$, the restriction map

$$\mathrm{Hom}_{gr}(\mathbb{G}_{m|S_{\lambda_1}}, \mathbb{G}_{m|S_{\lambda_1}}) \longrightarrow \mathrm{Hom}_{gr}(\mathbb{G}_{m|S_{\lambda_2}}, \mathbb{G}_{m|S_{\lambda_2}})$$

is an isomorphism.

Moreover for the extensions group we have

Proposition 4.4. *For any $\lambda \in \pi R \setminus \{0\}$, any S-action of $\mathbb{G}_m$ on $\mathcal{G}^{(\lambda)}$ is trivial. Moreover*

$$\mathrm{Ext}^1(\mathbb{G}_m, \mathcal{G}^{(\lambda)}) = 0$$

Proof. See [18, I 1.6, II 1.4]. □

We also want to recall what happens to the extensions group when $\lambda \in R^*$, i.e. $\mathcal{G}^{(\lambda)} \simeq \mathbb{G}_m$.

Proposition 4.5. *For any $\mu \in R \setminus \{0\}$, any action of $\mathcal{G}^{(\mu)}$ on $\mathbb{G}_m$ is trivial. Moreover*

$$\mathrm{Ext}^1(\mathcal{G}^{(\mu)}, \mathbb{G}_m) = 0.$$

Proof. See [18, I 1.5, I 2.7] □

We now consider the case $\mu, \lambda \in \pi R \setminus \{0\}$. Any action of $\mathcal{G}^{(\mu)}$ on $\mathcal{G}^{(\lambda)}$ is trivial ([18, I 1.6]). For any flat R-scheme X let us consider the exact sequence on the fppf site X_{fl}

$$0 \longrightarrow \mathcal{G}^{(\lambda)} \xrightarrow{\alpha^\lambda} \mathbb{G}_m \longrightarrow i_* \mathbb{G}_{m,X_\lambda} \longrightarrow 0, \tag{3}$$

where i denotes the closed immersion $X_\lambda = X \otimes_R (R/\lambda R) \hookrightarrow X$ (see [20, 1.2]). We observe that by definitions we have that

$$\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) = \{F(S) \in (R/\lambda R[S, \frac{1}{1+\mu S}])^* | F(S)F(T) = F(S+T+\mu ST)\}$$

If we apply the functor $\mathrm{Hom}(\cdot, \mathbb{G}_m)$ to the sequence (3) we obtain, in particular, a map

$$\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \xrightarrow{\alpha} \mathrm{Ext}^1(\mathcal{G}^{(\mu)}, \mathcal{G}^{(\lambda)}).$$

given by

$$F \longmapsto \mathcal{E}^{(\mu,\lambda;F)},$$

where

$$\mathcal{E}^{(\mu,\lambda;F)}$$

is a smooth affine commutative group defined as follows: let $\tilde{F}(S) \in R[S]$ be a lifting of $F(S)$, then

$$\mathcal{E}^{(\mu,\lambda;F)} = \mathrm{Spec}(R[S_1, S_2, \frac{1}{1+\mu S_1}, \frac{1}{\tilde{F}(S_1)+\lambda S_2}])$$

(1) law of multiplication

$$\begin{aligned} S_1 \longmapsto & S_1 \otimes 1 + 1 \otimes S_1 + \mu S_1 \otimes S_1 \\ S_2 \longmapsto & S_2 \otimes \tilde{F}(S_1) + \tilde{F}(S_1) \otimes S_2 + \lambda S_2 \otimes S_2 + \\ & \frac{\tilde{F}(S_1) \otimes \tilde{F}(S_1) - \tilde{F}(S_1 \otimes 1 + 1 \otimes S_1 + \mu S_1 \otimes S_1)}{\lambda} \end{aligned}$$

(2) unit

$$S_1 \longmapsto 0$$

$$S_2 \longmapsto \frac{1 - \tilde{F}(0)}{\lambda}$$

(3) inverse

$$S_1 \longmapsto -\frac{S_1}{1+\mu S_1}$$

$$S_2 \longmapsto \frac{\frac{1}{\tilde{F}(S_1)+\lambda S_2} - \tilde{F}(-\frac{S_1}{1+\mu S_1})}{\lambda}$$

We moreover define the following homomorphisms of group schemes

$$\mathcal{G}^{(\lambda)} = \mathrm{Spec}(R[S, (1+\lambda S)^{-1}]) \longrightarrow \mathcal{E}^{(\mu,\lambda;F)}$$

by

$$S_1 \longmapsto 0$$

$$S_2 \longmapsto S + \frac{1 - \tilde{F}(0)}{\lambda}$$

and

$$\mathcal{E}^{(\mu,\lambda;F)} \longrightarrow \mathcal{G}^{(\mu)} = \mathrm{Spec}(R[S, \frac{1}{1+\mu S}])$$

by

$$S \longrightarrow S_1.$$

It is easy to see that

$$0 \longrightarrow \mathcal{G}^{(\lambda)} \longrightarrow \mathcal{E}^{(\mu,\lambda;F)} \longrightarrow \mathcal{G}^{(\mu)} \longrightarrow 0 \tag{4}$$

is exact. A different choice of the lifting $\tilde{F}(S)$ gives an isomorphic extension. We recall the following theorem.

Theorem 4.6. *For any $\lambda, \mu \in \pi R \setminus \{0\}$, the map*

$$\alpha : \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \longrightarrow \mathrm{Ext}^1(\mathcal{G}^{(\mu)}, \mathcal{G}^{(\lambda)})$$

is a surjective morphism of groups. And $\ker(\alpha)$ is generated by the class of $1+\mu S$. In particular any extension of $\mathcal{G}^{(\mu)}$ by $\mathcal{G}^{(\lambda)}$ is commutative.

Proof. [17, §3]. □

We now define some spaces which had been used by Sekiguchi and Suwa to describe $\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$ and, by the above result, $\mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$. See [22] for details.

Definition 4.7. For any ring A, let $W_n(A)$ be the ring of Witt vectors of length n and $W(A)$ the ring of infinite Witt vectors. We define

$$\widehat{W}_n(A) = \Big\{ (a_0, \dots, a_n) \in W_n(A) | a_i \text{ is nilpotent for any } i \text{ and } a_i = 0 \text{ for all but a finite number of } i \Big\}$$

and

$$\widehat{W}(A) = \Big\{ (a_0, \dots, a_n, \dots) \in W(A) | a_i \text{ is nilpotent for any } i \text{ and } a_i = 0 \text{ for all but a finite number of } i \Big\}.$$

We recall the definition of the so-called Witt-polynomial: for any $r \geq 0$ it is

$$\Phi_r(T_0, \dots, T_r) = T_0^{p^r} + pT_1^{p^{r-1}} + \dots + p^r T_r.$$

Then the following maps are defined:

- Verschiebung

$$V : W_n(A) \longrightarrow W_{n+1}(A)$$
$$(a_0, \dots, a_n) \longmapsto (0, a_0, \dots, a_n)$$

- Generalization of Frobenius

$$\mathrm{F} : W_{n+1}(A) \longrightarrow W_n(A)$$
$$(a_0, \dots, a_n) \longmapsto (F_0(\mathbf{T}), F_1(\mathbf{T}), \dots, F_n(\mathbf{T}))$$

where the polynomials $F_r(\mathbf{T}) = F_r(T_0, \dots, T_r) \in \mathbb{Q}[T_0, \dots, T_{r+1}]$ are defined inductively by

$$\Phi_r(F_0(\mathbf{T}), F_1(\mathbf{T}), \dots, F_r(\mathbf{T})) = \Phi_{r+1}(T_0, \dots, T_{r+1}).$$

If $p=0\in A$ then F is the usual Frobenius. The subring $\widehat{W}(A)$ is stable respect to these maps.

For any morphism $G:\widehat{W}(A)\longrightarrow\widehat{W}(A)$ we will set $\widehat{W}(A)^G:=\ker G$. And for any $a\in A$ we denote the element $(a,0,0,\dots,0,\dots)\in W(A)$ by $[a]$.

We recall the following standard result about Witt vectors.

Lemma 4.8. *Let $S_r[\mathbf{T},\mathbf{U}]\in\mathbb{Z}[\mathbf{T},\mathbf{U}]$ such that, if $\boldsymbol{a},\boldsymbol{b}\in W(A)$, then*

$$\boldsymbol{a}+\boldsymbol{b}=(S_0[\boldsymbol{a},\boldsymbol{b}],\dots,S_r[\boldsymbol{a},\boldsymbol{b}],\dots)$$

If T_i and U_i have weight p^i then $S_r[\mathbf{T},\mathbf{U}]$ is isobaric of weight p^r.

The following lemma will be useful later.

Lemma 4.9. *Let $\lambda\in R$. If $\boldsymbol{a}=(a_0,a_1,\dots),\boldsymbol{b}=(b_0,b_1,\dots)\in\widehat{W}(R/\lambda R)^{\mathrm{F}}$ then*

$$\boldsymbol{a}+\boldsymbol{b}=(a_0+b_0,a_1+b_1,\dots,a_i+b_i,\dots)$$

Proof. We suppose that $\boldsymbol{a}+\boldsymbol{b}=(c_0,c_1,\dots,c_i,\dots)$. By the previous lemma we have that $c_r(\boldsymbol{a},\boldsymbol{b})$ is isobaric of weight p^r. It is a standard result that

$$c_r(\boldsymbol{a},\boldsymbol{b})=a_r+b_r+c_r'((a_0,a_1,\dots,a_{r-1}),(b_0,b_1,\dots,b_{r-1})).$$

for some polynomial $c_r'(S_0,\dots,S_{r-1},T_0,\dots,T_{r-1})$. Clearly $c_r'(\boldsymbol{a},\boldsymbol{b})$ is isobaric of weight p^r, too. Hence $\deg(c_r')\geq p$.

Let $\tilde{a_i},\tilde{b_i}\in R$ be liftings of a_i and b_i, respectively. For any $r\geq1$, up to changing $\boldsymbol{a}$ with $\boldsymbol{b}$, we can suppose that $v(\tilde{a_k})=\min\{v(\tilde{a_i}),v(\tilde{b_i})|i=0,\dots,r-1\}$, for some $0\leq k\leq r-1$. Since $\deg c_r'\geq p$ then $v(c_r'(\tilde{\boldsymbol{a}},\tilde{\boldsymbol{b}}))\geq pv(\tilde{a}_k)$. But $v(\tilde{a}_k^p)\geq v(\lambda)$ since $\mathrm{F}(\boldsymbol{a})=0$. Hence $c_r'(\boldsymbol{a},\boldsymbol{b})=0\in R/\lambda R$. So

$$\boldsymbol{a}+\boldsymbol{b}=(a_0+b_0,a_1+b_1,\dots,a_i+b_i,\dots)$$

□

We now recall the definition of the Artin-Hasse exponential series

$$E_p(T):=\exp\left(\sum_{r\geq0}\frac{T^{p^r}}{p^r}\right)=\prod_{r=0}^{\infty}\exp\left(\frac{T^{p^r}}{p^r}\right)\in\mathbb{Z}_{(p)}[[T]].$$

Sekiguchi and Suwa introduced a deformation of the Artin-Hasse exponential map in [22]. By the well known formula $\lim_{\mu\to0}(1+\mu x)^{\frac{\alpha}{\mu}}=\exp(\alpha x)$, it can be seen that $(1+\mu x)^{\frac{\alpha}{\mu}}$ is a deformation of $\exp(\alpha x)$. From this point of view they defined the formal power series $E_p(U,\Lambda;T)\in\mathbb{Q}[U,\Lambda][[T]]$ by

$$E_p(U,\Lambda;T):=(1+\Lambda T)^{\frac{U}{\Lambda}}\prod_{r=1}^{\infty}(1+\Lambda^{p^r}T^{p^r})^{\frac{1}{p^r}((\frac{U}{\Lambda})^{p^r}-(\frac{U}{\Lambda})^{p^{r-1}})}$$

They proved that $E_p(U,\Lambda;T)$ has in fact its coefficients in $\mathbb{Z}_{(p)}[U,\Lambda]$. It is possible to show ([22, 2.4]) that

$$E_p(U,\Lambda;T)=\begin{cases}\prod_{(i,p)=1}E_p(U\Lambda^{i-1}T^i)^{\frac{(-1)^{i-1}}{i}}, & \text{if } p>2;\\ \prod_{(i,2)=1}E_p(U\Lambda^{i-1}T^i)^{\frac{1}{i}}\left[\prod_{(i,2)=1}E_p(U\Lambda^{2i-1}T^{2i})^{\frac{1}{i}}\right]^{-1}, & \text{if } p=2.\end{cases}$$

Let A be a $\mathbb{Z}_{(p)}$-algebra and $a,\mu\in A$. We define $E_p(a,\mu;T)$ as $E_p(U,\Lambda;T)$ evaluated at $U=a$ and $\Lambda=\mu$.

Example 4.10. It is easy to see that $E_p(a,0;T)=E_p(aT)$ and $E_p(\mu,\mu;T)=1+\mu T$. Moreover if $a^p=\mu^{p-1}a\in A$ then $(\frac{a}{\mu})^{p^r}-(\frac{a}{\mu})^{p^{r-1}}=0$ for $r\geq1$. Hence

$$E_p(a,\mu;T)=(1+\mu T)^{\frac{a}{\mu}}=1+\sum_{i=1}^{p-1}\frac{\prod_{k=0}^{i-1}(a-k\mu)}{i!}T^i.$$

In particular if $\mu = 0$ and $a^p = 0 \in A$ then

$$E_p(a, 0; T) = \sum_{i=0}^{p-1} \frac{a^i}{i!} T^i.$$

If $\boldsymbol{a} = (a_0, a_1, a_2, \dots) \in W(A)$ we define the formal power series

$$E_p(\boldsymbol{a}, \mu; T) = \prod_{k=0}^{\infty} E_p(a_k, \mu^{p^k}; T^{p^k}). \tag{5}$$

The following result gives an explicit description of $\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|A}, \mathbb{G}_{m|A})$.

Theorem 4.11. *Let A be a $\mathbb{Z}_{(p)}$-algebra and $\mu \in A$ a nilpotent element. The homomorphism*

$$\begin{aligned} \xi^0_A : \widehat{W}(A)^{\mathrm{F}-[\mu^{p-1}]} &\longrightarrow \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|A}, \mathbb{G}_{m|A}) \\ \boldsymbol{a} &\longmapsto E_p(\boldsymbol{a}, \mu; S) \end{aligned}$$

is bijective.

Proof. [22, 2.19.1]. □

And 4.6 and 4.11 give the following:

Corollary 4.12. *For any $\lambda, \mu \in \pi R \setminus \{0\}$ the map*

$$\begin{aligned} \alpha \circ \xi^0_{R/\lambda R} : \widehat{W}(R/\lambda R)^{\mathrm{F}-[\mu^{p-1}]} / < 1 + \mu T > &\longrightarrow \mathrm{Ext}^1(\mathcal{G}^{(\mu)}, \mathbb{G}_m) \\ \boldsymbol{a} &\longmapsto \mathcal{E}^{(\lambda, \mu; E_p(\boldsymbol{a}, \lambda; S))} \end{aligned}$$

is an isomorphism.

We now describe some natural maps through these identifications. Consider the isogeny

$$\psi_{\mu,1} : \mathcal{G}^{(\mu)} \longrightarrow \mathcal{G}^{(\mu^p)}.$$

Let us now suppose that $p > 2$. Then we have that, if $p^2 \equiv 0 \mod \lambda$,

$$\psi^*_{\mu,1} : \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu^p)}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \longrightarrow \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$$

is given by

$$\boldsymbol{a} \longmapsto [\frac{p}{\mu^{p-1}}]\boldsymbol{a} + V(\boldsymbol{a}) \tag{6}$$

(see [22, 1.4.1 and 3.8]).

For $p = 2$ the situation is slightly different. Let us define a variant of the Verschiebung as follows. Define polynomials

$$\tilde{V}_r(\mathbf{T}) = \tilde{V}_r(T_0, \dots, T_r) \in \mathbb{Q}[T_0, \dots, T_r]$$

inductively by $\tilde{V}_0 = 0$ and

$$\Phi_r(\tilde{V}_0(\mathbf{T}), \dots, \tilde{V}_r(\mathbf{T})) = p^{p^r} \Phi_{r-1}(T_0, \dots, T_{r-1})$$

for $r \geq 1$. Then we have that (with possibly $2^2 \not\equiv 0 \mod \lambda$)

$$\psi^*_{\mu,1} : \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu^2)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \longrightarrow \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$$

is given by

$$\boldsymbol{a} \longmapsto [\frac{2}{\mu}]\boldsymbol{a} + V(\boldsymbol{a}) + \tilde{V}(\boldsymbol{a})$$

(see [22, 3.8]).

For simplicity, to avoid to use this description of $\psi^*_{\mu,1}$, we will consider sometimes only the case $p>2$.

Consider the morphism

$$
\begin{aligned}
p: \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) &\longrightarrow \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}}) \\
F(S) &\longmapsto F(S)^p
\end{aligned} \tag{7}
$$

This morphism is such that

$$\psi_{\lambda,1_*}\circ\alpha = \alpha\circ p.$$

Let $\boldsymbol{a}\in (\widehat{W}(R/\lambda R))^{\mathrm{F}-[\mu^{p-1}]}$. Take any lifting $\tilde{\boldsymbol{a}}\in W(R)$. Using the identifications of 4.11 the morphism p above is given by

$$\boldsymbol{a}\longmapsto p\tilde{\boldsymbol{a}} \tag{8}$$

(see [22, 4.6]). We will sometimes simply write $p\boldsymbol{a}$.

4.3. **Two exact sequences.** The main tools which we will use to calculate the extensions of $G_{\lambda,1}$ by $G_{\mu,1}$ are two exact sequences. We recall them in this subsection. See (9) and (12) below. First of all we prove that any action of $G_{\mu,1}$ on $G_{\lambda,1}$ is trivial.

Lemma 4.13. *Let $\varphi: G\longrightarrow H$ be an S-morphism of affine S-groups. Assume that G is flat over S. Then $\varphi=0$ if and only if the generic fiber $\varphi_K=0$.*

Proof. [18, 1.1]. □

Lemma 4.14. *Every action of $G_{\mu,1}$ on $G_{\lambda,1}$ is trivial.*

Proof. Giving an action of $G_{\lambda,1}$ on $G_{\mu,1}$ is the same as giving a morphism $G_{\mu,1}\longrightarrow Aut_R(G_{\lambda,1})$. If we consider the generic fiber we have a morphism

$$\mu_{p,K}\longrightarrow Aut_K(\mu_{p,K}).$$

The last one is the étale group scheme $(\mathbb{Z}/p\mathbb{Z})^*_K$. It is a group scheme of order $p-1$. So any morphism $\mu_{p,K}\longrightarrow Aut_K(\mu_{p,K})$ is trivial. Applying 4.13 we have the thesis. □

In the following, all the actions will be supposed trivial. Applying now the functor Ext to the following exact sequence of group schemes

$$(\Lambda): \qquad 0\longrightarrow G_{\lambda,1}\xrightarrow{i}\mathcal{G}^{(\lambda)}\xrightarrow{\psi_{\lambda,1}}\mathcal{G}^{(\lambda^p)}\longrightarrow 0,$$

we obtain

$$
\begin{aligned}
0\longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1},\mathcal{G}^{(\lambda^p)}) &\xrightarrow{\delta'} \mathrm{Ext}^1(G_{\mu,1},G_{\lambda,1})\xrightarrow{i_*} \\
&\longrightarrow \mathrm{Ext}^1(G_{\mu,1},\mathcal{G}^{(\lambda)})\xrightarrow{\psi_{\lambda,1_*}}\mathrm{Ext}^1(G_{\mu,1},\mathcal{G}^{(\lambda^p)}).
\end{aligned} \tag{9}
$$

We remark that δ' is injective since

$$\psi_{\lambda,1_*}:\mathrm{Hom}_{gr}(G_{\mu,1},\mathcal{G}^{(\lambda)})\longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1},\mathcal{G}^{(\lambda^p)})$$

is the zero morphism. Indeed since G is flat over R, then by 4.13,

$$\mathrm{Hom}_{gr}(G_{\mu,1},\mathcal{G}^{(\lambda)})\hookrightarrow \mathrm{Hom}_{gr}(\mu_{p,K},\mathbb{G}_{mK})\simeq\mathbb{Z}/p\mathbb{Z}.$$

And it is easy to verify that

$$\mathrm{Hom}_{gr}(G_{\mu,1},\mathcal{G}^{(\lambda)})=\begin{cases}\mathbb{Z}/p\mathbb{Z}, & \text{if } \lambda\mid\mu\\ 0, & \text{if } \lambda\nmid\mu\end{cases} \tag{10}$$

Let us write $G_{\mu,1}=\mathrm{Spec}(R[S]/(\frac{(1+\mu S)^p-1}{\mu^p}))$. If $\lambda\mid\mu$ the group is formed by the morphisms given by $\sigma_i: S\longmapsto\frac{(1+\mu S)^i-1}{\lambda}$ with $i\in\mathbb{Z}/p\mathbb{Z}$. The map $(\psi_{\lambda,1})_*:\mathrm{Hom}_{gr}(G_{\mu,1},\mathcal{G}^{(\lambda)})\longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1},\mathcal{G}^{(\lambda^p)})$ is moreover nothing else but the multiplication by p. So it is clearly zero.

The map

$$\delta' : \mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda^p)}) \longrightarrow \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1}) \tag{11}$$

is defined by

$$\sigma_i \longmapsto (\sigma_i)^*(\Lambda),$$

where $(\sigma_i)^*(\Lambda)$ is explicitly

$$\mathrm{Spec}(R[S_1,S_2]/(\frac{(1+\mu S_1)^p-1}{\mu^p}, \frac{(1+\lambda S_2)^p-(1+\mu S_1)^i}{\lambda^p}),$$

with the maps

$$\begin{aligned} G_{\lambda,1} &\longrightarrow \sigma_i^*(\Lambda)\\ S_1 &\longmapsto 0\\ S_2 &\longmapsto S \end{aligned}$$

and

$$\begin{aligned} \sigma_i^*(\Lambda) &\longrightarrow G_{\mu,1}\\ S &\longmapsto S_1 \end{aligned}$$

The structure of group scheme on $\sigma_i^*(\Lambda)$ is the unique one which makes the map

$$\begin{aligned} \sigma_i^*(\Lambda) &\longrightarrow \mu_{p^2} = \mathrm{Spec}(R[Z_1,Z_2]/(Z_1^p-1, Z_2^p-Z_1^i))\\ Z_1 &\longmapsto 1+\mu S_1\\ Z_2 &\longmapsto 1+\lambda S_2 \end{aligned}$$

a morphism of group schemes.

As remarked in [18, 4.4], there is the following long exact sequence

$$\begin{aligned} 0 \longrightarrow \quad &\mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda')}) \longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m) \xrightarrow{r_{\lambda'}} \mathrm{Hom}_{gr}(G_{\mu,1|S_{\lambda'}}, \mathbb{G}_{m|S_{\lambda'}}) \xrightarrow{\delta}\\ &\longrightarrow \mathrm{Ext}^1(G_{\mu,1}, \mathcal{G}^{(\lambda')}) \xrightarrow{\alpha_*^{\lambda'}} \mathrm{Ext}^1(G_{\mu,1}, \mathbb{G}_m) \longrightarrow \mathrm{Ext}^1(G_{\mu,1|S_{\lambda'}}, \mathbb{G}_{m|S_{\lambda'}}). \end{aligned} \tag{12}$$

We so have

$$\ker \alpha_*^{\lambda'} \simeq Im\delta \simeq \mathrm{Hom}_{gr}(G_{\mu,1|S_{\lambda'}}, \mathbb{G}_{m|S'_\lambda})/r_{\lambda'}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)). \tag{13}$$

We remark that by (10), setting $\lambda' = 1$, it follows that

$$\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m) \simeq \mathbb{Z}/p\mathbb{Z}$$

and the group is formed by the morphisms $S \longmapsto (1+\mu S)^i$. While, by (10), $\mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda')}) \simeq \mathbb{Z}/p\mathbb{Z}$ if $\lambda'|\mu$ and it is 0 otherwise. Hence, by (12), if $\lambda'|\mu$ then $r_{\lambda'}$ is the zero morphism, otherwise $r_{\lambda'}$ is an isomorphism. Hence, by (13),

$$\ker \alpha_*^{\lambda'} \simeq \mathrm{Hom}_{gr}(G_{\mu,1|S_{\lambda'}}, \mathbb{G}_{m|S_{\lambda'}})/ < 1+\mu S > . \tag{14}$$

In the following we give a more explicit description of the main ingredients of the exact sequences (9) and (12).

4.4. **Explicit description of** $\mathrm{Hom}_{gr}(G_{\mu,1|S_\lambda}, \mathbb{G}_{m|S_\lambda})$**.** First we consider the simplest cases. If $\lambda \in \pi R$,

$$\mathrm{Hom}_{gr}(\mu_{p|S_\lambda}, \mathbb{G}_{m|S_\lambda}) = \{S^i \in (R/\lambda R)[S, 1/S] | i \in \mathbb{Z}/p\mathbb{Z}\}. \tag{15}$$

While if $\lambda \in R^*$ we have $S_\lambda = \emptyset$ and $\mathrm{Hom}_{gr}(G_{\mu,1|S_\lambda}, \mathbb{G}_{m|S_\lambda}) = \{1\}$.

Now we study $\mathrm{Hom}_{gr}(G_{\mu,1|S_\lambda}, \mathbb{G}_{m|S_\lambda})$ for $\mu, \lambda \in \pi R \setminus \{0\}$.

Proposition 4.15. *Let $\lambda, \mu \in \pi R \setminus \{0\}$. The map*

$$i^* : \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$$

induced by

$$i : G_{\mu,1} \hookrightarrow \mathcal{G}^{(\mu)}$$

is surjective. If $p > 2$, $\xi^0_{R/\lambda}$, defined in 4.11, induces an isomorphism

$$\widehat{W}(R/\lambda R)^{\mathrm{F}-[\mu^{p-1}]}/\left\{[\frac{p}{\mu^{p-1}}]\boldsymbol{b} + V(\boldsymbol{b}) | \boldsymbol{b} \in \widehat{W}(R/\lambda R)^{\mathrm{F}-[\mu^{p(p-1)}]}\right\} \longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$$

Proof. We have by definitions that

$$\mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) = \{F(S) \in \left(R/\lambda R[S]/(\frac{(1+\mu S)^p - 1}{\mu^p})\right)^* | \\ F(S)F(T) = F(S+T+\mu ST)\}$$

and

$$\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) = \{F(S) \in \left(R/\lambda R[S, \frac{1}{1+\mu S}]\right)^* | \\ F(S)F(T) = F(S+T+\mu ST)\}.$$

Since $(G_{\mu,1})_k$ is isomorphic to α_p or $\mathbb{Z}/p\mathbb{Z}$ then the group $\mathrm{Hom}_{gr}((G_{\mu,1})_k, \mathbb{G}_{m,k})$ is trivial. So $F(S) \equiv 1 \mod \pi$. Moreover any $F(S) \in (R/\lambda R)[S]/(\frac{(1+\mu S)^p-1}{\mu^p})$ such that $F(S) \equiv 1 \mod \pi$ is invertible. The same is true in $\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$ since $\mathcal{G}^{(\mu)}_k \simeq \mathbb{G}_a$. We now say that F satisfies condition $(\sharp)$ if

$F(S) \equiv 1 \mod \pi$;
$F(S)F(T) = F(S+T+\mu ST)$.

Then

$$\mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) = \{F(S) \in R/\lambda R[S]/(\frac{(1+\mu S)^p - 1}{\mu^p}) | F(S) \text{ satifies } (\sharp)\}$$

and

$$\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) = \{F(S) \in R/\lambda R[S, \frac{1}{1+\mu S}] | F(S) \text{ satifies } (\sharp)\}.$$

Any $F \in R/\lambda R[S]/(\frac{(1+\mu S)^p-1}{\mu^p})$ can be represented by a polynomial of degree $p-1$. And if it satisfies $(\sharp)$, it also satisfies $(\sharp)$ in $R/\lambda R[S, \frac{1}{1+\mu S}]$.

So

$$i^* : \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$$

is surjective.

Now, by the exact sequence

$$(\Lambda') \qquad 0 \longrightarrow G_{\mu,1} \xrightarrow{i} \mathcal{G}^{(\mu)} \xrightarrow{\psi_{\mu,1}} \mathcal{G}^{(\mu^p)} \longrightarrow 0$$

over S_λ, we have the long exact sequence of cohomology

$$0 \longrightarrow \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu^p)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \xrightarrow{\psi^*_{\mu,1}} \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \xrightarrow{i^*} \\ \longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \xrightarrow{\delta''} \mathrm{Ext}^1(\mathcal{G}^{(\mu^p)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \longrightarrow \dots$$

By 4.11 we have that

$$\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \simeq \widehat{W}(R/\lambda R)^{F-[\mu^{p-1}]}$$

and, by (6),

$$\psi^*_{\mu,1}(\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu^p)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})) \simeq \left\{[\frac{p}{\mu^{p-1}}]\boldsymbol{b} + V(\boldsymbol{b}) | \boldsymbol{b} \in \widehat{W}(R/\lambda R)^{\mathrm{F}-[\mu^{p(p-1)}]}\right\}.$$

Therefore the proposition is proved. $\square$

We now give a more explicit description of $\mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda},\mathbb{G}_{m|S_\lambda})$.

Proposition 4.16. *If $\lambda,\mu\in R$ with $v(p)\geq(p-1)v(\mu)>0$ and $v(p)\geq v(\lambda)$, then*

$$\mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda},\mathbb{G}_{m|S_\lambda})=\{E_p(a,\mu;S)=1+\sum_{i=1}^{p-1}\frac{\prod_{k=0}^{i-1}(a-k\mu)}{i!}S^i$$
$$\text{s.t. } a\in R/\lambda R \text{ and } a^p=\mu^{p-1}a\in R/\lambda R\}$$

Remark 4.17. In [16, 3.5], an inductive formula for the coefficients of the polynomials $F(T)\in\mathrm{Hom}(\mathcal{G}^{(\mu)}{}_{|S_\lambda},\mathbb{G}_{m|S_\lambda})$ is given. If we consider only polynomials of degree less or equal to $p-1$, it coincides with (18). But for the reader's convenience, we prefer to give here a direct proof of this formula.

Remark 4.18. If $v(\mu)\geq v(\lambda)$ then

$$\mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda},\mathbb{G}_{m|S_\lambda})=\{\sum_{i=0}^{p-1}\frac{a^i}{i!}T^i|a^p=0\}=\{E_p(aT)|a^p=0\}$$

Proof. As seen in 4.15

$$\mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda},\mathbb{G}_{m|S_\lambda})=\{F(S)=\sum_{i=0}^{p-1}a_iS^i\in R/\lambda R[S]/(\frac{(1+\mu S)^p-1}{\mu^p})$$
$$\text{s.t. } F(S)\equiv 1 \mod \pi \text{ and } F(S)F(T)=F(S+T+\mu ST)\}.$$

Now

$$\begin{aligned}F(S+T+\mu ST)&=\sum_{i=0}^{p-1}a_i(S+T+\mu ST)^i\\&=\sum_{i=0}^{p-1}\sum_{j=0}^{i}\sum_{k=0}^{j}\binom{i}{j}\binom{j}{k}\mu^{i-j}a_iS^{k+i-j}T^{i-k}\\&=\sum_{r=0}^{p-1}\sum_{l=0}^{p-1}\sum_{\max\{r,l\}\leq i\leq r+l}\binom{i}{2i-(r+l)}\binom{2i-(r+l)}{i-l}\mu^{r+l-i}a_iS^rT^l\end{aligned}\tag{16}$$

and

$$F(S)F(T)=\sum_{r=0}^{p-1}\sum_{l=0}^{p-1}a_ra_lS^rT^l.\tag{17}$$

So we have the equality if and only if

$$\begin{aligned}a_ra_l&=\sum_{\max\{r,l\}\leq i\leq r+l}\binom{i}{2i-(r+l)}\binom{2i-(r+l)}{i-l}\mu^{r+l-i}a_i\\&=\sum_{\max\{r,l\}\leq i\leq r+l}\frac{i!}{(r+l-i)!(i-l)!(i-r)!}\mu^{r+l-i}a_i\end{aligned}\tag{18}$$

for any $0\leq r,l\leq p-1$. Clearly $a_0=1$.

We now have the following lemma:

Lemma 4.19. *For any $\mu,\lambda\in\pi R\setminus\{0\}$, the following statements are equivalent*

i) $a_r=\frac{\prod_{k=0}^{r-1}(a_1-k\mu)}{r!}$ *for any* $1\leq r\leq p-1$ *and* $\prod_{k=0}^{p-1}(a_1-k\mu)=0$;
ii) $a_{r-1}a_1=(r-1)\mu a_{r-1}+ra_r$ *for any* $1\leq r\leq p-1$;
iii) $a_ra_l=\sum_{\max\{r,l\}\leq i\leq r+l}\frac{i!}{(r+l-i)!(i-l)!(i-r)!}\mu^{r+l-i}a_i$ *for any* $1\leq l,r\leq p-1$.

Proof. In the following we use the convention that $a_i = 0$ if $i > p-1$.

$i) \Leftrightarrow ii)$. It is clear that
$$a_{r-1}a_1 = (r-1)\mu a_{r-1} + ra_r$$
is equivalent to $a_r = a_{r-1}\frac{a_1-\mu(r-1)}{r}$, if $r < p$, and $a_{p-1}(a_1 - \mu(p-1)) = 0$. An easy induction shows that this is equivalent to
$$a_r = \frac{\prod_{k=0}^{r-1}(a_1 - k\mu)}{r!}$$
if $r < p-1$ and
$$\prod_{k=0}^{p-1}(a_1 - k\mu) = 0.$$

$ii) \Leftarrow iii)$. It is obvious.

$ii) \Rightarrow iii)$. We will prove it by induction on l. By hypothesis $a_{r-1}a_1 = (r-1)\mu a_{r-1} + ra_r$ for any r. We now suppose that $iii)$ is true for $k \leq l-1$ for any r. Then we will prove it is also true for l for any r. We can clearly suppose $l \leq r$, otherwise, up to a change of l with r, we can conclude by induction. We have
$$\begin{aligned}
a_r a_l &\overset{ii)}{=} a_r\left(a_{l-1}\frac{a_1-\mu(l-1)}{l}\right)\\
&= (a_r a_{l-1})\frac{a_1-\mu(l-1)}{l}\\
&\overset{induct.}{=} \left(\sum_{r\leq i\leq r+l-1}\frac{i!}{(r+l-i-1)!(i-l-1)!(i-r)!}\mu^{r+l-i-1}a_i\right)\frac{a_1-\mu(l-1)}{l}\\
&\overset{induct.}{=} \sum_{r\leq i\leq r+l-1}\frac{i!}{(r+l-i-1)!(i-l-1)!(i-r)!}\mu^{r+l-i-1}\\
&\quad\left(\frac{\mu(i-l+1)a_i + (i+1)a_{i+1}}{l}\right)\\
&= \frac{r!}{l!(r+1-l)!}\mu^l(r+1-l)a_r +\\
&\quad + \sum_{r+1\leq i\leq r+l-1}\left(\frac{i!}{(r+l-i)!(i-l)!(i-r-1)!l}\mu^{r+l-i} +\right.\\
&\quad \left. + \frac{i!(i-l+1)}{(r+l-i)!(i-l+1)!(i-r)!l}\mu^{r+l-i}\right)a_i + \frac{(r+l-1)!(r+l)}{r!l!}a_{r+l}\\
&= \sum_{r\leq i\leq r+l}\frac{i!}{(r+l-i)!(i-l)!(i-r)!}\mu^{r+l-i}a_i.
\end{aligned}$$
□

We come back to the proof of the proposition. In $R/\lambda R$ the condition
$$\prod_{k=0}^{p-1}(a_1 - k\mu) = 0$$
is equivalent to $a_1^p = \mu^{p-1}a_1$. Indeed we have the following equality in $\mathbb{Z}/p\mathbb{Z}[S]$
$$\prod_{k=0}^{p-1}(S-k) = S^p - S,$$
since these polynomials have the same zeros. Since $p = 0 \in R/\lambda R$, then
$$\prod_{k=0}^{p-1}(a_1 - k\mu) = a_1^p - \mu^{p-1}a_1.$$

By the lemma and 4.10 the thesis follows. □

We now essentially rewrite 4.19 in a more expressive form.

Corollary 4.20. *Let $\lambda,\mu\in\pi R\setminus\{0\}$ and let $F(S)=\sum_{i=0}^{p-1}a_iS^i\in R/\lambda R[S]$ be a polynomial of degree less than or equal to $p-1$. Then the following statements are equivalent*

(i) $F(S)F(T)-a_0^2=F(S+T+\mu ST)-a_0$

(ii) $F(S)a_1=F'(S)(1+\mu S)$ *where F' is the formal derivative of F.*

Remark 4.21. Let us suppose $v(\mu)\geq v(\lambda)$. This corollary, together with 4.16, says that the solution of the differential equation in $R/\lambda R[S]/(\frac{(1+\mu S)^p-1}{\mu^p})$

$$\begin{cases} F'(S)=aF(S),\\ F(0)=1\end{cases}$$

has as unique solution $F(S)=E_p(aS)=\sum_{i=0}^{p-1}\frac{a^i}{i!}S^i$ and $a^p=0$.

Proof. By (18), we have that 4.19(iii) is equivalent to

$$F(S)F(T)-a_0^2=F(S+T+\mu ST)-a_0. \tag{19}$$

If we put $l=1$ in (18), we obtain the coefficient of T in both members of (19). This means that 4.19(ii) is equivalent to

$$F(S)a_1=F'(S)(1+\mu S).$$

Then their equivalence comes from 4.19.

□

When $v(\mu)\geq v(\lambda)$, putting together 4.15 and 4.16, we have a simpler description of $\mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}},\mathbb{G}_{m|S_\lambda})$.

Corollary 4.22. *Let $p>2$. Let $\lambda,\mu\in R$ with $v(p)\geq(p-1)v(\mu)>0$ and $v(\mu)\geq v(\lambda)>0$. Then we have the following isomorphism of groups*

$$(\xi^0_{R/\lambda R})_p:(R/\lambda R)^{\mathrm{F}}\longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}},\mathbb{G}_{m|S_\lambda})$$

given by

$$a\longmapsto E_p(aS).$$

Moreover the restriction map

$$i^*:\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda},\mathbb{G}_{m|S_\lambda})\simeq\widehat{W}(R/\lambda R)^{\mathrm{F}}\longrightarrow\mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}},\mathbb{G}_{m|S_\lambda})\simeq(R/\lambda R)^{\mathrm{F}}$$

is given, in terms of Witt vectors, by

$$\boldsymbol{a}=(a_0,a_1,\ldots,0,0,0,\ldots)\longmapsto\sum_{i=0}^{\infty}(-1)^i(\frac{p}{\mu^{p-1}})^ia_i$$

Proof. We first remark that the restriction of the Teichmüller map

$$T:(R/\lambda R)^{\mathrm{F}}\longrightarrow\widehat{W}(R/\lambda R)^{\mathrm{F}},$$

given by

$$a\longmapsto[a],$$

is a morphism of groups. This follows from 4.9. Moreover, if we consider the isomorphism

$$\xi^0_{R/\lambda R}:\widehat{W}(R/\lambda R)^{\mathrm{F}}\longrightarrow\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda},\mathbb{G}_{m|S_\lambda})$$

and

$$i^*:\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda},\mathbb{G}_{m|S_\lambda})\longrightarrow\mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}},\mathbb{G}_{m|S_\lambda}),$$

we have

$$i^*\circ\xi^0_{R/\lambda R}\circ T=(\xi^0_{R/\lambda R})_p.$$

So $(\xi^0_{R/\lambda R})_p$ is a morphism of groups. It is surjective by 4.16 and, by 4.15, its kernel is

$$T((R/\lambda R)^{\mathrm{F}})\cap\left\{[\frac{p}{\mu^{p-1}}]\boldsymbol{b}+V(\boldsymbol{b})|\boldsymbol{b}\in\widehat{W}(R/\lambda R)^{\mathrm{F}}\right\}.$$

Let us now suppose that there exists $\boldsymbol{b} = (b_0, b_1, \dots) \in \widehat{W}(R/\lambda R)^{\mathrm{F}}$ and $a \in (R/\lambda R)^{\mathrm{F}}$ such that $[\frac{p}{\mu^{p-1}}]\boldsymbol{b} + V(\boldsymbol{b}) = [a]$. It follows by the definition of Witt vector ring that

$$[\frac{p}{\mu^{p-1}}]\boldsymbol{b} = (\frac{p}{\mu^{p-1}}b_0, \dots, (\frac{p}{\mu^{p-1}})^{p^j}b_j, \dots), \tag{20}$$

and

$$[a] - V(\boldsymbol{b}) = (a_0, -b_0, -b_1, \dots). \tag{21}$$

Since $\boldsymbol{b} \in \widehat{W}(R/\lambda R)$, there exists $r \geq 0$ such that $b_j = 0$ for any $j \geq r$. Moreover, comparing (20) and (21) it follows

$$\begin{aligned}
(\frac{p}{\mu^{p-1}})^{p^j} b_{j+1} &= -b_j \quad \text{ for } j \geq 0\\
(\frac{p}{\mu^{p-1}})^{p} b_0 &= a.
\end{aligned}$$

Hence $b_j = a = 0$ for any $j \geq 0$. It follows that $(\xi^0_{R/\lambda R})_p$ is injective.

We now prove the second part of the statement. First of all we remark that for any $\boldsymbol{a} = (a_0, \dots, a_j, \dots) \in \widehat{W}(R/\lambda R)^{\mathrm{F}}$ we have

$$\boldsymbol{a} = \sum_{j=0}^{\infty} V^j([a_j]).$$

It is clear that for any $a \in R/\lambda R$ we have $i^*([a]) = a$. While, by 4.15, it follows that $i^*V(\boldsymbol{b}) = -i^*([\frac{p}{\mu^{p-1}}]\boldsymbol{b})$ for any $\boldsymbol{b} \in \widehat{W}(R/\lambda R)^{\mathrm{F}}$. Hence $i^*V^j(\boldsymbol{b}) = (-1)^j i^*([(\frac{p}{\mu^{p-1}})^j]\boldsymbol{b})$ for any $j \geq 1$. From these facts it follows that

$$\begin{aligned}
i^*(\boldsymbol{a}) &= i^*(\sum_{j=0}^{\infty} V^j([a_j]))\\
&= \sum_{j=0}^{\infty} (i^*(V^j([a_j])))\\
&= \sum_{j=0}^{\infty} (-1)^j (\frac{p}{\mu^{p-1}})^j a_j.
\end{aligned}$$

□

4.5. **Explicit description of δ.** The map

$$\delta : \mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \longrightarrow \mathrm{Ext}^1(G_{\mu,1}, \mathcal{G}^{(\lambda)})$$

can also be explicitly described. We have the following commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \arrow[r] \arrow[d, "\alpha"] & \mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \arrow[r] \arrow[d, "\delta"] & 0\\
\mathrm{Ext}^1(\mathcal{G}^{(\mu)}, \mathcal{G}^{(\lambda)}) \arrow[r, "i^*"] & \mathrm{Ext}^1(G_{\mu,1}, \mathcal{G}^{(\lambda)}) &
\end{tikzcd}$$

where the first horizontal map is surjective by 4.15. So, given

$$F(S) \in \mathrm{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}),$$

we can choose a representant in $\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$ which we denote again by $F(S)$ for simplicity. Then δ is defined by

$$F(S) \longmapsto \widetilde{\mathcal{E}}^{(\mu,\lambda;F)} := i^*(\mathcal{E}^{(\mu,\lambda;F)}) = i^*(\alpha(F(S))).$$

If $\tilde{F}(S) \in R[S]$ is any lifting then it is defined, as a scheme, by

$$\widetilde{\mathcal{E}}^{(\mu,\lambda;F)} = \mathrm{Spec}\left(R[S_1, S_2, (\tilde{F}(S_1)+\lambda S_2)^{-1}]/\frac{(1+\mu S_1)^p - 1}{\mu^p}\right).$$

This extension does not depend on the choice of the lifting since the same is true for $\mathcal{E}^{(\mu,\lambda;F)}$.

So, by (12), we see that $\ker(\alpha_*^\lambda) \subseteq \mathrm{Ext}^1(G_{\mu,1}, \mathcal{G}^{(\lambda)})$ is nothing else but the group $\{\widetilde{\mathcal{E}}^{(\mu,\lambda;F)}\}$. We recall that, by (13), for any $\lambda' \in R$,

$$\ker \alpha_*^{\lambda'} \simeq \mathrm{Hom}_{gr}(G_{\mu,1_{|S_{\lambda'}}}, \mathbb{G}_{m|S_{\lambda'}})/r_{\lambda'}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)).$$

We have therefore proved the following proposition.

Proposition 4.23. *Let $\lambda, \mu \in R \setminus \{0\}$ with $v(p) \geq (p-1)v(\mu)$. Then δ induces an isomorphism*

$$\begin{aligned}\mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}}, \mathbb{G}_{m|S_\lambda})/r_{\lambda'}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)) &\longrightarrow \{\widetilde{\mathcal{E}}^{(\mu,\lambda;F)}\}\\ F(S) &\longmapsto \widetilde{\mathcal{E}}^{(\mu,\lambda;F)}\end{aligned}$$

Remark 4.24. As remarked in §4.3, if $\lambda' \mid \mu$ then

$$r_{\lambda'}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)) = 0,$$

otherwise

$$r_{\lambda'}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)) \simeq < 1+\mu S > \simeq \mathbb{Z}/p\mathbb{Z}.$$

Example 4.25.

a) Let us suppose $v(\mu) = 0$ and $v(\lambda) > 0$. Since, by (15) and the previous remark,

$$\mathrm{Hom}_{gr}(\mu_{p|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \simeq r_\lambda(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)) \simeq \mathbb{Z}/p\mathbb{Z}$$

then $\{\widetilde{\mathcal{E}}^{(\mu,\lambda;F)}\} = 0$.

b) Let us suppose $v(\lambda) = 0$. Since $S_\lambda = \emptyset$, then $\{\widetilde{\mathcal{E}}^{(\mu,\lambda;F)}\} = 0$.

4.6. **Interpretation of** $\mathrm{Ext}^1(G_{\mu,1}, \mathbb{G}_m)$**.** First of all, we briefly recall a useful spectral sequence . Let $\mathcal{E}xt^i(G,H)$ denote the fppf-sheaf on $Sch_{/S}$, associated to the presheaf $X \longmapsto \mathrm{Ext}^i(G \times_S X, H \times_S X)$. Then we have a spectral sequence

$$E_2^{ij} = H^i(S, \mathcal{E}xt^j(G,H)) \Rightarrow \mathrm{Ext}^{i+j}(G,H),$$

which in low degrees gives

$$\begin{aligned}0 \longrightarrow H^1(S, \mathcal{E}xt^0(G,H)) \longrightarrow \mathrm{Ext}^1(G,H) \longrightarrow H^0(S, \mathcal{E}xt^1(G,H)) \longrightarrow\\ \longrightarrow H^2(S, \mathcal{E}xt^0(G,H)) \longrightarrow \mathrm{Ext}^2(G,H).\end{aligned} \tag{22}$$

All the groups of cohomology are calculated in the fppf topology. Moreover $H^1(S, \mathcal{E}xt^0(G,H))$ is isomorphic to the subgroup of $\mathrm{Ext}^1(G,H)$ formed by the extensions E which split over some faithfully flat affine S-scheme of finite type (cf. [4, III 6.3.6]). We suppose that G acts trivially on H, then $\mathcal{E}xt^0(G,H) = \mathcal{H}om_{gr}(G,H)$. We will consider the case $H = \mathbb{G}_m$ and G a finite flat group scheme. In this case, $\mathcal{E}xt^0(G, \mathbb{G}_m)$ is by definition the Cartier dual of G, denoted by $G^\vee$. We recall the following result which will play a role in the description of extensions of $G_{\mu,1}$ by $G_{\lambda,1}$ (see 4.39 below).

Theorem 4.26. *Let G be a commutative finite flat group scheme over S. Then the canonical map*

$$H^1(S, G^\vee) \longrightarrow \mathrm{Ext}^1(G, \mathbb{G}_m)$$

is bijective.

Proof. This is a Theorem of S.U. Chase. For a proof see [25]. We stress that he proves $\mathcal{E}xt^1(G, \mathbb{G}_m) = 0$, then he applies (22). We remark that he proves everything in the fpqc site. However the same proof works in the fppf site. $\square$

We apply this result to $G = G_{\lambda,1}$. We have that the map

$$H^1(S, G^\vee_{\lambda,1}) \longrightarrow \mathrm{Ext}^1(G_{\lambda,1}, \mathbb{G}_m)$$

is an isomorphism. Moreover the following is true.

Proposition 4.27. *Let X be a normal integral scheme. For any finite and flat commutative group scheme G over X,*

$$i^* : H^1(X, G) \longrightarrow H^1(\mathrm{Spec}(K(X)), G_{|K(X)})$$

is injective, where $i : \mathrm{Spec}(K(X)) \longrightarrow X$ is the generic point.

Proof. A sketch of the proof has been suggested to us by F. Andreatta. We recall that for any commutative group scheme G' over a scheme X' we have that $H^1(X', G')$ is a group and it classifies the G'-torsors over X'. Suppose there exists a G-torsor $f : Y \longrightarrow X$ such that $i^*f : i^*Y \to \mathrm{Spec}(K(X))$ is trivial. This means there exists a section s of i^*f. We consider the scheme Y_0 which is the closure of $s(\mathrm{Spec}(K(X)))$ in Y. Then $f_{|Y_0} : Y_0 \longrightarrow X$ is a finite birational morphism with X a normal integral scheme. So, by Zariski's Main Theorem ([7, 4.4.6]), we have that $f_{|Y_0}$ is an open immersion, and so it is an isomorphism. So we have a section of f and Y is a trivial G-torsor. □

Remark 4.28. The hypothesis G finite and X normal are necessary. For the first it is sufficient to observe that any $\mathbb{G}_m$-torsor is trivial on $\mathrm{Spec}(K(X))$. For the second one, consider $X = \mathrm{Spec}(k[x,y]/(x^p - y^{p+1})) = \mathrm{Spec}(A)$, with k any field of characteristic $p > 0$, and Y the α_p-torsor $\mathrm{Spec}(A[T]/(T^p - y))$. Generically this torsor is trivial since we have $y = (\frac{x}{y})^p$. But Y is not trivial since y is not a p-power in A.

Corollary 4.29. *Let X be a normal integral scheme. Let $f : Y \longrightarrow X$ be a morphism with a rational section and let $g : G \longrightarrow G'$ a map of finite and flat commutative group schemes over X, which is an isomorphism over* $\mathrm{Spec}(K(X))$. *Then*

$$f^*g_* : H^1(X, G) \longrightarrow H^1(Y, G'_Y)$$

is injective.

Proof. By hypothesis $\mathrm{Spec}(K(X)) \longrightarrow X$ factorizes through $f : Y \longrightarrow X$. If $i : \mathrm{Spec}(K(X)) \longrightarrow X$, we have

$$i_* : H^1(X, G) \xrightarrow{g_*} H^1(X, G') \xrightarrow{f^*} H^1(Y, G'_Y) \longrightarrow H^1(\mathrm{Spec}(K(X)), G_{K(X)}).$$

Therefore, by the previous proposition, it follows that

$$H^1(X, G) \longrightarrow H^1(Y, G'_Y)$$

is injective. □

Remark 4.30. The previous corollary can be applied, for instance, to the case $f = \mathrm{id}_X$ or to the case $f : U \longrightarrow X$ an open immersion and $g = \mathrm{id}_G$. Roberts ([11, p. 692]) has proved the corollary in the case $f = \mathrm{id}_X$, with $X = \mathrm{Spec}(A)$ and A the integer ring of a local number field.

By 4.26 and 4.27 we obtain the following result.

Corollary 4.31. *Let G be a commutative finite flat group scheme over S. The restriction map*

$$\mathrm{Ext}^1(G, \mathbb{G}_m) \longrightarrow \mathrm{Ext}^1(G_K, \mathbb{G}_{m|K})$$

is injective.

Let us consider a commutative finite and flat group scheme G of order n. We also consider the n^{th} power map $n : \mathbb{G}_m \longrightarrow \mathbb{G}_m$. It induces a morphism $n_* : \mathrm{Ext}^1(G, \mathbb{G}_m) \longrightarrow \mathrm{Ext}^1(G, \mathbb{G}_m)$. We have the following commutative diagram

$$\begin{tikzcd} H^1(S, G^\vee) \arrow[r] \arrow[d, "n_*"] & \mathrm{Ext}^1(G, \mathbb{G}_m) \arrow[d, "n_*"] \\ H^1(S, G^\vee) \arrow[r] & \mathrm{Ext}^1(G, \mathbb{G}_m), \end{tikzcd}$$

where the horizontal maps are isomorphisms by 4.39. We remark that $n_* : H^1(S, G^\vee) \longrightarrow H^1(S, G^\vee)$ is the zero morphism since the map $n_* : G^\vee \longrightarrow G^\vee$, induced by $n : \mathbb{G}_m \longrightarrow \mathbb{G}_m$, is the zero morphism. This proves the following lemma.

Lemma 4.32. *Let G be a commutative finite and flat group scheme of order n. Then*

$$n_* : \mathrm{Ext}^1(G, \mathbb{G}_m) \longrightarrow \mathrm{Ext}^1(G, \mathbb{G}_m)$$

is the zero morphism.

4.7. **Description of** $\mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$**.** We finally have all the ingredients to give a description of the group $\mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$. In particular we will focus on the extensions which are isomorphic, as group schemes, to $\mathbb{Z}/p^2\mathbb{Z}$ on the generic fiber.

First of all we remark that if $v(\mu_1) = v(\mu_2)$ and $v(\lambda_1) = v(\lambda_2)$ then

$$\mathrm{Ext}^1(G_{\mu_1,1}, G_{\lambda_1,1}) \simeq \mathrm{Ext}^1(G_{\mu_2,1}, G_{\lambda_2,1}).$$

Indeed we know, by hypothesis, that there exist two isomorphisms $\psi_1 : G_{\lambda_1,1} \longrightarrow G_{\lambda_2,1}$ and $\psi_2 : G_{\mu_2,1} \longrightarrow G_{\mu_1,1}$. Then we have that

$$(\psi_1)_* \circ (\psi_2)^* : \mathrm{Ext}^1(G_{\mu_1,1}, G_{\lambda_1,1}) \longrightarrow \mathrm{Ext}^1(G_{\mu_2,1}, G_{\lambda_2,1})$$

is an isomorphism.

We now recall what happens if $v(\mu) = v(\lambda) = 0$. In this case we have the following result.

Proposition 4.33. *Let A be a d.v.r or a field. Then there exists an exact sequence*

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Ext}^1_A(\mu_p, \mu_p) \longrightarrow H^1(\mathrm{Spec}(A), \mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

Proof. The proposition is proved in [15, 3.7] when A a is d.v.r. The same proof works when A is a field. □

Let us define the extension of μ_p by μ_p

$$\mathcal{E}_{i,A} = \mathrm{Spec}(A[S_1, S_2]/(S_1^p - 1, \frac{S_2^p}{S_1^i} - 1)).$$

It is the kernel of the morphism $(\mathbb{G}_m)^2 \longrightarrow (\mathbb{G}_m)^2$ given by $(S_1, S_2) \longrightarrow (S_1^p, S_1^{-1}S_2^p)$ Then the group $\mathbb{Z}/p\mathbb{Z}$ in the above proposition is formed by the extensions $\mathcal{E}_{i,A}$.

Definition 4.34. Let $F \in \mathrm{Hom}(G_{\mu,1_{|S_\lambda}}, \mathbb{G}_{m|S_\lambda})$, $j \in \mathbb{Z}/p\mathbb{Z}$ such that

$$F(S)^p(1 + \mu S)^{-j} = 1 \in \mathrm{Hom}(G_{\mu,1_{|S_{\lambda^p}}}, \mathbb{G}_{m|S_{\lambda^p}}).$$

Let $\tilde{F}(S) \in R[S]$ be a lifting of F. We denote by $\mathcal{E}^{(\mu,\lambda;F,j)}$ the subgroup scheme of $\mathcal{E}^{(\mu,\lambda;F)}$ given on the level of schemes by

$$\mathcal{E}^{(\mu,\lambda;F,j)} = \mathrm{Spec}\left(R[S_1, S_2]/(\frac{(1 + \mu S_1)^p - 1}{\mu^p}, \frac{(\tilde{F}(S_1) + \lambda S_2)^p(1 + \mu S_1)^{-j} - 1}{\lambda^p})\right).$$

We moreover define the following homomorphisms of group schemes

$$G_{\lambda,1} \longrightarrow \mathcal{E}^{(\mu,\lambda;F,j)}$$

by

$$S_1 \longmapsto 0$$

$$S_2 \longmapsto S + \frac{1-\tilde{F}(0)}{\lambda}$$

and

$$\mathcal{E}^{(\mu,\lambda;F,j)} \longrightarrow G_{\mu,1}$$

by

$$S \longrightarrow S_1.$$

It is easy to see that

$$0 \longrightarrow G_{\lambda,1} \longrightarrow \mathcal{E}^{(\mu,\lambda;F)} \longrightarrow G_{\mu,1} \longrightarrow 0$$

is exact. A different choice of the lifting $\tilde{F}(S)$ gives an isomorphic extension. It is easy to see that $(\mathcal{E}^{(\mu,\lambda;F,j)})_K \simeq (\mathbb{Z}/p^2\mathbb{Z})_K$, as a group scheme, if $j \neq 0$ and $(\mathcal{E}^{(\mu,\lambda;F,0)})_K \simeq (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})_K$.

Remark 4.35. In the above definition the integer j is uniquely determined by $F \in \mathrm{Hom}(G_{\mu,1_{|S_\lambda}}, \mathbb{G}_{m|S_\lambda})$ if and only if $\lambda^p \nmid \mu$.

From the exact sequence over S_λ

$$0 \longrightarrow G_{\mu,1} \xrightarrow{i} \mathcal{G}^{(\mu)} \xrightarrow{\psi_{\mu,1}} \mathcal{G}^{(\mu^p)} \longrightarrow 0$$

we have that

$$\ker\left(i^* : \mathrm{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \longrightarrow \mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}}, \mathbb{G}_{m|S_\lambda})\right) = \psi_{\mu,1_*}\mathrm{Hom}_{gr}(\mathcal{G}^{(\mu^p)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \tag{23}$$

So let $F(S) \in \mathrm{Hom}(G_{\mu,1_{|S_{\lambda^p}}}, \mathbb{G}_{m|S_{\lambda^p}})$. By 4.15 we can choose a representant of $F(S)$ in $\in \mathrm{Hom}(\mathcal{G}^{(\mu)}{}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}})$ which we denote again $F(S)$ for simplicity. Therefore, by (23), we have that $F(S)^p(1+\mu S)^{-j} = 1 \in \mathrm{Hom}(G_{\mu,1_{|S_{\lambda^p}}}, \mathbb{G}_{m|S_{\lambda^p}})$ is equivalent to saying that there exists $G \in \mathrm{Hom}(\mathcal{G}^{(\mu^p)}{}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}})$ with the property that $F(S)^p(1+\mu S)^{-j} = G(\frac{(1+\mu S)^p-1}{\mu^p}) \in \mathrm{Hom}(\mathcal{G}^{(\mu)}{}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}})$. This implies that $\mathcal{E}^{(\mu,\lambda;F,j)}$ can be seen as the kernel of the isogeny

$$\psi^j_{\mu,\lambda,F,G} : \mathcal{E}^{(\mu,\lambda;F)} \longrightarrow \mathcal{E}^{(\mu^p,\lambda^p;G)}$$

$$S_1 \longmapsto \frac{(1+\mu S_1)^p - 1}{\mu^p}$$

$$S_2 \longmapsto \frac{(\tilde{F}(S_1)+\lambda S_2)^p(1+\mu S_1)^{-j} - \tilde{G}(\frac{(1+\mu S_1)^p-1}{\mu^p})}{\lambda^p}$$

where $\tilde{F}, \tilde{G} \in R[T]$ are liftings of F and G.

As remarked in 4.18, if $v(\mu) \geq v(\lambda)$ we can suppose

$$\tilde{F}(S) = \sum_{i=0}^{p-1} \frac{a^i}{i!} S^i$$

with $a^p \equiv 0 \mod \lambda$.

Example 4.36. This example has been the main motivation for our definition of the group schemes $\mathcal{E}^{(\mu,\lambda;F,j)}$. Let us define

$$\eta=\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\lambda_{(2)}^k.$$

We remark that $v(\eta)=v(\lambda_{(2)})$. We consider

$$F(S)=E_p(\eta S)=\sum_{k=1}^{p-1}\frac{(\eta S)^k}{k!}$$

It has been shown in [22, §5] that, using our notation,

$$\mathbb{Z}/p^2\mathbb{Z}\simeq\mathcal{E}^{(\lambda_{(1)},\lambda_{(1)};E_p(\eta S),1)}.$$

A similar description of $\mathbb{Z}/p^2\mathbb{Z}$ was independently found by Green and Matignon ([5]).

Example 4.37. It is easy to see that the group scheme $G_{\lambda,2}$ is isomorphic to

$$\mathcal{E}^{(\lambda^p,\lambda;1,1)}.$$

Moreover if we have an extension of type $\mathcal{E}^{(\mu,\lambda;F,j)}$ with $F(S)=1$ then $v(\mu)\geq pv(\lambda)$. Indeed we have that

$$\mathcal{E}^{(\mu,\lambda;1,j)}=\operatorname{Spec}\left(A[S_1,S_2]/\left(\frac{(1+\mu S_1)^p-1}{\mu^p},\frac{(1+\lambda S_2)^p(1+\mu S_1)^{-j}-1}{\lambda^p}\right)\right).$$

Since $(1+\lambda S_2)^p=1\in\operatorname{Hom}_{gr}(G_{\mu,1_{|S_{\lambda^p}}},\mathbb{G}_{m|S_\lambda^p})$ then

$$(1+\lambda S_2)^p(1+\mu S_1)^{-j}=1\in\operatorname{Hom}_{gr}(G_{\mu,1_{|S_{\lambda^p}}},\mathbb{G}_{m|S_{\lambda^p}})$$

if and only if $v(\mu)\geq pv(\lambda)$. In particular we remark that, in such a case, $v(\lambda)\leq v(\lambda_{(2)})$. Otherwise

$$pv(\lambda)>pv(\lambda_{(2)})=v(\lambda_{(1)})\geq v(\mu),$$

which is not possible.

Let us define, for any $\mu,\lambda\in R$ with $v(\mu),v(\lambda)\leq v(\lambda_{(1)})$, the group

$$rad_{p,\lambda}(<1+\mu S>):=\Big\{(F(S),j)\in\operatorname{Hom}_{gr}(G_{\mu,1_{|S_\lambda}},\mathbb{G}_{m|S_\lambda})\times\mathbb{Z}/p\mathbb{Z}\text{ such that}$$

$$F(S)^p(1+\mu S)^{-j}=1\in\operatorname{Hom}(G_{\mu,1_{|S_{\lambda^p}}},\mathbb{G}_{m|S_{\lambda^p}})\Big\}/<(1+\mu S,0)>.$$

We define

$$\beta:rad_{p,\lambda}(<1+\mu S>)\longrightarrow\operatorname{Ext}^1(G_{\mu,1},G_{\lambda,1})$$

by

$$(F(S),j)\longmapsto\mathcal{E}^{(\mu,\lambda;F(S),j)}$$

We remark that the image of β is the set $\{\mathcal{E}^{(\mu,\lambda;F(S),j)}\}$.

Lemma 4.38. *β is a morphism of groups. In particular the set $\{\mathcal{E}^{(\mu,\lambda;F(S),j)}\}$ is a subgroup of* $\operatorname{Ext}^1(G_{\mu,1},G_{\lambda,1})$.

Proof. Let $i:G_{\lambda,1}\longrightarrow\mathcal{G}^{(\lambda)}$. We remark that

$$i_*(\beta(F,j))=i_*(\mathcal{E}^{(\mu,\lambda;F(S),j)})=\tilde{\mathcal{E}}^{(\mu,\lambda;F)}=\delta(F)$$

for any $(F,j)\in rad_{p,\lambda}(<1+\mu S>)$. Moreover by construction

$$(\mathcal{E}^{(\mu,\lambda;F(S),j)})_K=(\mathcal{E}_j)_K\in\operatorname{Ext}^1(\mu_{p,K},\mu_{p,K}).$$

Let $(F_1, j_1), (F_2, j_2) \in rad_{p,\lambda}(< 1 + \mu S >)$. Then

$$i_*(\beta(F_1, j_1) + \beta(F_2, j_2) - \beta(F_1 + F_2, j_1 + j_2)) = \delta(F_1) + \delta(F_2) - \delta(F_1 + F_2) = 0 \tag{24}$$

since δ is a morphism of groups. And

$$(\beta(F_1, j_1) + \beta(F_2, j_2) - \beta(F_1 + F_2, j_1 + j_2))_K = \mathcal{E}_{j_1,K} + \mathcal{E}_{j_2,K} - \mathcal{E}_{j_1+j_2,K} = 0, \tag{25}$$

since $\mathbb{Z}/p\mathbb{Z} \simeq \mathrm{Ext}^1(\mu_{p,K}, \mu_{p,K})$ through the map $j \mapsto \mathcal{E}_{j,K}$. By (24) it follows that

$$\beta(F_1, j_1) + \beta(F_2, j_2) - \beta(F_1 + F_2, j_1 + j_2) \in \ker i_*.$$

and then, by (9) and (11), we have

$$\beta(F_1, j_1) + \beta(F_2, j_2) - \beta(F_1 + F_2, j_1 + j_2) = (\sigma_j)^*\Lambda.$$

for some $j \in \mathbb{Z}/p\mathbb{Z}$. By (25) it follows that

$$((\sigma_j)^*\Lambda)_K = \mathcal{E}_{j,K} = 0,$$

therefore $j = 0$. So β is a morphism of groups. The last assertion is clear. □

We now give a description of $\mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$.

Theorem 4.39. *Suppose that $\lambda, \mu \in R$ with $v(\lambda_{(1)}) \geq v(\lambda), v(\mu)$. The following sequence*

$$\begin{aligned} 0 \longrightarrow rad_{p,\lambda}(< 1 + \mu S >) \xrightarrow{\beta} \quad & \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1}) \xrightarrow{\alpha_*^\lambda \circ i_*} \\ & \longrightarrow \ker\left(H^1(S, G_{\mu,1}^\vee) \longrightarrow H^1(S_\lambda, G_{\mu,1}^\vee)\right) \end{aligned}$$

is exact. In particular β induces an isomorphism $rad_{p,\lambda}(< 1 + \mu S >) \simeq \{\mathcal{E}^{(\mu,\lambda;F,j)}\}$.

Proof. Using (12) and 4.23, we consider the following commutative diagram

(26)

$$\begin{tikzcd} 0 \arrow[r] & \{\widetilde{\mathcal{E}}^{(\mu,\lambda;F)}\} \arrow[r] \arrow[d, "\widetilde{\psi_{\lambda,1_*}}"] & \mathrm{Ext}^1(G_{\mu,1}, \mathcal{G}^{(\lambda)}) \arrow[r, "\alpha_*^\lambda"] \arrow[d, "\psi_{\lambda,1_*}"] & \mathrm{Ext}^1(G_{\mu,1}, \mathbb{G}_m) \arrow[r] \arrow[d, "p_*"] & \mathrm{Ext}^1(G_{\mu,1|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \arrow[d, "p_*"] \\ 0 \arrow[r] & \{\widetilde{\mathcal{E}}^{(\mu,\lambda^p;G)}\} \arrow[r] & \mathrm{Ext}^1(G_{\mu,1}, \mathcal{G}^{(\lambda^p)}) \arrow[r, "\alpha_*^{\lambda^p}"] & \mathrm{Ext}^1(G_{\mu,1}, \mathbb{G}_m) \arrow[r] & \mathrm{Ext}^1(G_{\mu,1|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \end{tikzcd}$$

The map $\widetilde{\psi_{\lambda,1_*}}$, induced by $\psi_{\lambda,1_*} : \mathrm{Ext}^1(G_{\mu,1}, \mathcal{G}^{(\lambda)}) \longrightarrow \mathrm{Ext}^1(G_{\mu,1}, \mathcal{G}^{(\lambda^p)})$, is given by $\widetilde{\mathcal{E}}^{(\mu,\lambda;F)} \longmapsto \widetilde{\mathcal{E}}^{(\mu,\lambda^p;F^p)}$. Now, since $G_{\mu,1}$ is of order p then, $p_* : \mathrm{Ext}^1(G_{\mu,1}, \mathbb{G}_m) \to \mathrm{Ext}^1(G_{\mu,1}, \mathbb{G}_m)$ is the zero map (see 4.32). Moreover, by (22) and 4.26, we have the following situation

$$\begin{tikzcd} 0 \arrow[r] & H^1(S, G_{\mu,1}^\vee) \arrow[r] \arrow[d] & \mathrm{Ext}^1(G_{\mu,1}, \mathbb{G}_m) \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & H^1(S_\lambda, G_{\mu,1}^\vee) \arrow[r] & \mathrm{Ext}^1(G_{\mu,1|S_\lambda}, \mathbb{G}_{m|S_\lambda}) & \end{tikzcd}$$

which implies that $Im(\alpha_*^\lambda) \simeq \ker(H^1(S, G_{\mu,1}^\vee) \longrightarrow H^1(S_\lambda, G_{\mu,1}^\vee))$.

So applying the snake lemma to (26) we obtain

$$0 \longrightarrow \ker(\widetilde{\psi_{\lambda,1_*}}) \xrightarrow{\widetilde{\delta}} \ker(\psi_{\lambda,1_*}) \xrightarrow{\alpha_*^\lambda} \ker\left(H^1(S, G_{\mu,1}^\vee) \longrightarrow H^1(S_\lambda, G_{\mu,1}^\vee)\right). \tag{27}$$

We now divide the proof in some steps.

$\boxed{\text{Connection between } \ker(\widetilde{\psi_{\lambda,1_*}}) \text{ and } rad_{p,\lambda}(< 1 + \mu S >).}$ We are going to give the connection in the form of the isomorphism (31) below. We recall that, by (9), $i : G_{\lambda,1} \longrightarrow \mathcal{G}^{(\lambda)}$ induces an isomorphism

$$i_* : \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})/\delta'(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda^p)})) \longrightarrow \ker(\psi_{\lambda,1_*}); \tag{28}$$

for the definition of δ' see (11).

By 4.23 we have an isomorphism

$$\delta : \mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}}, \mathbb{G}_{m|S_\lambda})/r_{\lambda'}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)) \longrightarrow \{\widetilde{\mathcal{E}}^{(\mu,\lambda;F)}\}$$

Through this identification we can identify $\ker(\widetilde{\psi_{\lambda,1_*}})$ with

$$\left\{ F(S) \in \mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}}, \mathbb{G}_{m|S_\lambda}) | \exists i \in r_{\lambda^p}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)) \text{ such that} \right. \tag{29}$$
$$\left. F(S)^p(1+\mu S)^{-i} = 1 \in \mathrm{Hom}(G_{\mu,1_{|S_{\lambda^p}}}, \mathbb{G}_{m|S_{\lambda^p}}) \right\} / < 1+\mu S > .$$

Moreover

$$\widetilde{\delta} : \ker(\widetilde{\psi_{\lambda,1_*}}) \hookrightarrow \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})/\delta'(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda^p)})) \subseteq \mathrm{Ext}^1(G_{\mu,1}, \mathcal{G}^{(\lambda)}) \tag{30}$$

is defined by $\widetilde{\delta}(F) = \delta(F) = \widetilde{\mathcal{E}}^{(\mu,\lambda;F)}$.

We now define a morphism of groups

$$\iota : \ker(\widetilde{\psi_{\lambda,1_*}}) \longrightarrow r_{\lambda^p}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m))$$

as follows: for any $F(S) \in \ker(\widetilde{\psi_{\lambda,1_*}})$, $\iota(F) = i_F$ is the unique $i \in r_{\lambda^p}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m))$ such that $F(S)^p(1+\mu S)^{-i} = 1 \in \mathrm{Hom}(G_{\mu,1_{|S_{\lambda^p}}}, \mathbb{G}_{m|S_{\lambda^p}})$. The morphism of groups

$$\begin{aligned} \ker(\widetilde{\psi_{\lambda,1_*}}) \times \mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda^p)}) &\longrightarrow rad_{p,\lambda}(< 1+\mu S >) \\ (F, j) &\longmapsto (F, i_F + j) \end{aligned} \tag{31}$$

is an isomorphism. We prove only the surjectivity since the injectivity is clear. Now, if $\lambda^p \nmid \mu$ then $\mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda^p)}) = 0$ and $r_{\lambda^p}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)) = \mathbb{Z}/p\mathbb{Z}$. So, if $(F, j) \in rad_{p,\lambda}(< 1+\mu S >)$, then $j \in r_{\lambda^p}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m))$. So $i_F = j$. Hence $(F, 0) \mapsto (F, i_F) = (F, j)$. While if $\lambda^p \mid \mu$ then $\mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda^p)}) = \mathbb{Z}/p\mathbb{Z}$ and $r_{\lambda^p}(\mathrm{Hom}_{gr}(G_{\mu,1}, \mathbb{G}_m)) = 0$. Hence

$$\ker(\widetilde{\psi_{\lambda,1_*}}) = \left\{ F(S) \in \mathrm{Hom}_{gr}(G_{\mu,1_{|S_\lambda}}, \mathbb{G}_{m|S_\lambda}) | F(S)^p = 1 \in \mathrm{Hom}(G_{\mu,1_{|S_{\lambda^p}}}, \mathbb{G}_{m|S_{\lambda^p}}) \right\}.$$

Let us now take $(F, j) \in rad_{p,\lambda}(< 1+\mu S >)$. This means that

$$F(S)^p = (1+\mu S)^j = 1 \in \mathrm{Hom}(G_{\mu,1_{|S_{\lambda^p}}}, \mathbb{G}_{m|S_{\lambda^p}}).$$

Therefore $F(S) \in \ker(\widetilde{\psi_{\lambda,1_*}})$ and $i_F = 0$. So

$$(F, j) \longmapsto (F, i_F + j) = (F, j).$$

$\boxed{\text{Interpretation of } \beta.}$ We now define the morphism of groups

$$\begin{aligned} \varrho : \ker(\widetilde{\psi_{\lambda,1_*}}) &\longrightarrow \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1}) \\ F &\longmapsto \beta(F, i_F) = \mathcal{E}^{(\mu,\lambda;F,i_F)} \end{aligned}$$

We recall the definition of δ' given in (11):

$$\delta' : \mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda^p)}) \longrightarrow \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$$

is defined by $\delta'(\sigma_i) = \sigma_i^*(\Lambda)$. Then, under the isomorphism (31), we have

$$\beta = \varrho + \delta' : \ker(\widetilde{\psi_{\lambda,1_*}}) \times \mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda^p)}) \longrightarrow \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$$

$\boxed{\text{Injectivity of } \beta.}$ First of all we observe that $\widetilde{\delta}$ factors through ϱ, i.e.

$$\widetilde{\delta} = i_* \circ \varrho : \ker(\widetilde{\psi_{\lambda,1_*}}) \xrightarrow{\varrho} \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1}) \xrightarrow{i_*} \ker(\psi_{\lambda,1_*}). \tag{32}$$

Indeed

$$i_* \circ \varrho(F) = i_*(\mathcal{E}^{(\mu,\lambda;F,i_F)}) = \widetilde{\mathcal{E}}^{(\mu,\lambda,F)} = \widetilde{\delta}(F).$$

In particular, since $\tilde{\delta}$ is injective, ϱ is injective, too.

We now prove that $\beta = \varrho + \delta'$ is injective, too. By (28),

$$i_* \circ \delta' = 0.$$

Now, if $(\varrho + \delta')(F, \sigma_i) = 0$, then $\varrho(F) = -\delta'(\sigma_i)$. So

$$\widetilde{\delta}(F) = i_*(\varrho(F)) = i_*(-\delta'(\sigma_i)) = 0.$$

But $\widetilde{\delta}$ is injective, so $F = 1$. Hence $\delta'(\sigma_i) = 0$. But by (9), also δ' is injective. Then $\sigma_i = 0$.

$\boxed{\text{Calculation of } Im\beta.}$ We finally prove $Im(\varrho + \delta') = \ker(\alpha_*^\lambda \circ i_*)$. Since $\widetilde{\delta} = i_* \circ \varrho$, $\alpha_*^\lambda \circ \widetilde{\delta} = 0$ and $i_* \circ \delta' = 0$ then

$$\alpha_*^\lambda \circ i_* \circ (\varrho + \delta') = \alpha_*^\lambda \circ i_* \circ \varrho + \alpha_*^\lambda \circ (i_* \circ \delta') = \alpha_*^\lambda \circ i_* \circ \varrho = \alpha_*^\lambda \circ \widetilde{\delta} = 0.$$

So $Im(\varrho+\delta') \subseteq \ker(\alpha_*^\lambda \circ i_*)$. On the other hand, if $E \in \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$ is such that $\alpha_*^\lambda \circ i_*(E) = 0$, then, by (27), there exists $F \in \ker(\widetilde{\psi_{\lambda,1_*}})$ such that $i_*(E) = \widetilde{\delta}(F) = i_*(\varrho(F))$. Hence, by (28), $E - \varrho(F) \in Im(\delta')$. Therefore $Im(\varrho+\delta') = \ker(\alpha_*^\lambda \circ i^*)$. Moreover since $i_* : \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1}) \longrightarrow \ker(\psi_{\lambda,1_*})$ is surjective then $Im(\alpha_*^\lambda) = Im(\alpha_*^\lambda \circ i_*)$. We have so proved, using also (27), that the following sequence

$$0 \longrightarrow \ker(\widetilde{\psi_{\lambda,1_*}}) \times \mathrm{Hom}_{gr}(G_{\mu,1}, \mathcal{G}^{(\lambda^p)}) \xrightarrow{\varrho+\delta'} \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1}) \xrightarrow{\alpha_*^\lambda \circ i_*}$$
$$\longrightarrow \ker\left(H^1(S, G_{\mu,1}^\vee) \longrightarrow H^1(S_\lambda, G_{\mu,1}^\vee)\right)$$

is exact. Finally, by definitions, it follows that

$$\beta(rad_{p,\lambda}(< 1 + \mu S >)) = \{\mathcal{E}^{(\mu,\lambda;F,j)}\}.$$

$\square$

Example 4.40. Let us suppose $v(\lambda) = 0$. In such a case $rad_{p,\lambda}(< 1 + \mu T >) = \mathbb{Z}/p\mathbb{Z}$. Hence by the theorem we have

$$0 \longrightarrow \{\mathcal{E}^{(\mu,\lambda;1,j)} | j \in \mathbb{Z}/p\mathbb{Z}\} \longrightarrow \mathrm{Ext}^1(G_{\mu,1}, \mu_p) \longrightarrow H^1(S, G_{\mu,1}^\vee) \longrightarrow 0.$$

Example 4.41. Let us now suppose $v(\mu) = 0$ and $v(\lambda) > 0$. In such a case

$$\mathrm{Hom}_{gr}(\mu_{p|S_\lambda}, \mathbb{G}_{m|S_\lambda}) =< 1 + \mu T > .$$

Hence it is easy to see that

$$rad_{p,\lambda}(< 1 + \mu T >) = 0.$$

Therefore, by the theorem,

$$\mathrm{Ext}^1(\mu_p, G_{\lambda,1}) \longrightarrow \ker\left(H^1(S, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(S_\lambda, \mathbb{Z}/p\mathbb{Z})\right)$$

is an isomorphism.

Corollary 4.42. *Under the hypothesis of the theorem, any extension $E \in \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$ is of type $\mathcal{E}^{(\mu,\lambda;F,j)}$, up to an extension of R. In particular any extension is commutative.*

Proof. Let $E \in \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$. Suppose that $\alpha_*^\lambda(i_* E) = [S']$, with $S' \longrightarrow S$ a $G_{\mu,1}^\vee$-torsor. We consider the integral closure S'' of S in S'_K. Up to a localization (in the case $S'' \longrightarrow S$ is étale), we can suppose S'' local. So $S'' = \mathrm{Spec}(R'')$ where R'' is a noœtherian local integrally closed ring of dimension 1, i.e. a d.v.r. (see [2, 9.2]). Since $S''_K \simeq S'_K$, then $S'_K \times_K S''_K$ is a trivial E_K-torsor over S''_K. By 4.27 we have that $S' \times_S S''$ is a trivial E-torsor trivial over S''. So, if we make the base change $f : S'' \to S$, then $\alpha_*^\lambda(i_*(E_{S'})) = 0$. By 4.39, this implies that E'' is of type

$$\mathcal{E}^{(\mu,\lambda,F,j)}.$$

Hence any $E \in \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$ is a commutative group scheme over an extension R' of R. So it is a commutative group scheme over R.

□

Remark 4.43. Any R-group scheme of order p^2 is of type $\mathcal{E}^{(\mu,\lambda,F,j)}$, possibly after an extension of R. Indeed, up to an extension of R, the generic fiber of any R-group scheme is a constant group. Then the thesis follows from 4.1 and 4.42.

By 4.2 the extensions of $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$ over K, which are extensions of abstract groups, are classified by $H_0^2(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$ (see for instance [15, 2.7]). This group is formed by $\mathcal{E}_{j,K}$ with $j \in \mathbb{Z}/p\mathbb{Z}$. If $j \neq 0$ we have that $\mathcal{E}_{j,K}$ is isomorphic, as a group scheme, to $\mathbb{Z}/p^2\mathbb{Z}$, while if $j = 0$ it is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. We also define the following morphism of extensions

$$\begin{aligned} \alpha_{\mu,\lambda} : \mathcal{E}^{(\mu,\lambda;F,j)} &\longrightarrow \mathcal{E}_{j,R} \\ S_1 &\longmapsto 1 + \mu S_1 \\ S_2 &\longmapsto F(S_1) + \lambda S_2. \end{aligned} \tag{33}$$

It is an isomorphism on the generic fiber. Now, by the theorem, we get that $\mathcal{E}^{(\mu,\lambda;F,j)}$ are the only extensions which are isomorphic to $\mathcal{E}_{j,K}$ on the generic fiber.

Corollary 4.44. *The extensions of type $\mathcal{E}^{(\mu,\lambda;F,j)}$ are the only extensions $\mathcal{E} \in \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$ which are isomorphic, as extensions, to $\mathcal{E}_{j,K}$ on the generic fiber. In particular they are the unique finite and flat R-group schemes of order p^2 which are models of constant groups. More precisely, they are isomorphic on the generic fiber, as group schemes, to $\mathbb{Z}/p^2\mathbb{Z}$ if $j \neq 0$ and to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ if $j = 0$.*

Proof. As remarked above any $\mathcal{E}^{(\mu,\lambda;F,j)}$ has the properties of the statement. We now prove that they are the unique extensions of $G_{\mu,1}$ by $G_{\lambda,1}$ to have these properties. Let $\mathcal{E} \in \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$ be such that $\mathcal{E}_K \simeq \mathcal{E}_{j,K}$ as group schemes. By 4.26, 4.33 and 4.39 we have the following commutative diagram

$$\begin{array}{ccc} \mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1}) & \xrightarrow{\alpha_*^\lambda \circ i_*} & \ker\left(H^1(S, G_{\mu,1}^\vee) \longrightarrow H^1(S_\lambda, G_{\mu,1}^\vee)\right) \\ \downarrow & & \downarrow \\ \mathrm{Ext}^1_K(\mu_p, \mu_p) & \xrightarrow{\alpha_*^\lambda \circ i_*} & \mathrm{Ext}^1_K(\mu_p, \mathbb{G}_m) \simeq H^1(\mathrm{Spec}(K), \mathbb{Z}/p\mathbb{Z}) \longrightarrow 0 \end{array}$$

where the vertical maps are the restrictions to the generic fiber. Suppose now that $\mathcal{E}_K$ is of type $\mathcal{E}_{j,K}$. By 4.33 it follows that $\alpha_*^\lambda \circ i_*(\mathcal{E}_K) = 0$. Since the above diagram commutes, this means that $(\alpha_*^\lambda \circ i_*(\mathcal{E}))_K = 0$. By 4.27 we have that the second vertical map of the diagram is injective. This means that

$$\alpha_*^\lambda \circ i_*(\mathcal{E}) = 0.$$

So 4.39 implies that $\mathcal{E}$ is of type $\mathcal{E}^{(\mu,\lambda;F,j)}$. Now, if G is a model of a constant group, by 4.1 we have that G is an extension $\mathcal{E}$ of $G_{\mu,1}$ by $G_{\lambda,1}$. Moreover, since $\mathcal{E}_K$ is a constant group, then $\mathcal{E}_K \in \mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$. Therefore $\mathcal{E}_K \simeq \mathcal{E}_j$ for some j. So, by what we just proved, $\mathcal{E}$ is of type $\mathcal{E}^{(\mu,\lambda;F,j)}$. The last assertion is clear. □

4.8. $\mathrm{Ext}^1(G_{\mu,1}, G_{\lambda,1})$ **and the Sekiguchi-Suwa theory.** We now give a description of $\mathcal{E}^{(\mu,\lambda;F,j)}$ through the Sekiguchi-Suwa theory. We study separately the cases $\lambda \nmid \mu$ and $\lambda | \mu$.

Corollary 4.45. *Let $\mu, \lambda \in R$ be with $v(\lambda_{(1)}) \geq v(\lambda) > v(\mu)$. Then, no $\mathcal{E} \in \operatorname{Ext}^1(G_{\mu,1}, G_{\lambda,1})$ is a model of $(\mathbb{Z}/p^2\mathbb{Z})_K$. Moreover, if $p > 2$ and $v(\mu) > 0$, the group $\{\mathcal{E}^{(\mu,\lambda;F,j)}\}$ is isomorphic to*

$$\left\{ \boldsymbol{a} \in \widehat{W}(R/\lambda R)^{\mathrm{F}-[\mu^{p-1}]} | \exists \boldsymbol{b} \in \widehat{W}(R/\lambda^p R)^{\mathrm{F}-[\mu^{p(p-1)}]} \text{ such that} \right.$$

$$\left. p\boldsymbol{a} = [\frac{p}{\mu^{p-1}}]\boldsymbol{b} + V(\boldsymbol{b}) \in \widehat{W}(R/\lambda^p R) \right\} \Big/ < [\mu], \left\{ [\frac{p}{\mu^{p-1}}]\boldsymbol{b} + V(\boldsymbol{b}) | \boldsymbol{b} \in \widehat{W}(R/\lambda^p R)^{\mathrm{F}-[\mu^{p(p-1)}]} \right\} >,$$

through the map

$$\boldsymbol{a} \longmapsto \mathcal{E}^{(\mu,\lambda;E_p(\boldsymbol{a},\mu;S),0)}.$$

Remark 4.46. We know by 4.16, 4.15 and 4.10 that any element of the set defined above can be chosen of the type $[a]$ for some $a \in (R/\lambda R)^{\mathrm{F}-[\mu^{p-1}]}$. So, if we have two elements as above of the form $[a]$ and $[b]$ then $[a]+[b]=[c]$ for some $c \in (R/\lambda R)^{\mathrm{F}-[\mu^{p-1}]}$. We are not able to describe explicitly this element. If we were able to do it we could have a simpler description of the above set, as it happens in the case $v(\mu) \geq v(\lambda)$. We will see this in 4.47.

Proof. We now prove the first statement. We remark that by 4.44 it is sufficient to prove the statement only for the extensions in $\{\mathcal{E}^{(\mu,\lambda;F,j)}\}$. Let us consider the restriction map

$$r : \operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}}) \longrightarrow \operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}).$$

The morphism $p : \operatorname{Hom}_{gr}(\mathcal{G}^{(\mu)}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \longrightarrow \operatorname{Hom}_{gr}(\mathcal{G}^{(\mu)}{}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}})$ defined in (7) is given by $F(S) \mapsto F(S)^p$ and induces a map

$$\operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \xrightarrow{p} \operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}}).$$

Then

$$\operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \xrightarrow{p} \operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}}) \xrightarrow{r} \operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$$

is the trivial morphism. Indeed

$$(r \circ p)(F(S)) = F(S)^p \in \operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}),$$

which is zero by definition of group scheme morphisms and by the fact that $G_{\mu,1}$ has order p. Now let us take

$$F(S) \in rad_{p,\lambda}(< 1+\mu S >) \simeq \{\mathcal{E}^{(\mu,\lambda;F,j)}\}.$$

By definition

$$F(S)^p(1+\mu S)^{-j} = 1 \in \operatorname{Hom}(G_{\mu,1}{}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}}),$$

for some $j \in \mathbb{Z}/p\mathbb{Z}$. Hence

$$r(F(S)^p(1+\mu S)^{-j}) = (1+\mu S)^{-j} = 1 \in \operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}).$$

If $(\mathcal{E}^{(\mu,\lambda;F,j)})_K \simeq (\mathbb{Z}/p^2\mathbb{Z})_K$ then $j \neq 0$. Therefore

$$(1+\mu S)^{-j} = 1 \in \operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda})$$

means $v(\mu) \geq v(\lambda)$. So, if $v(\mu) < v(\lambda)$, necessarily $j = 0$. Hence

$$rad_{p,\lambda}(< 1+\mu S >) := \left\{ F(S) \in \operatorname{Hom}_{gr}(G_{\mu,1}{}_{|S_\lambda}, \mathbb{G}_{m|S_\lambda}) \text{ such that} \right.$$

$$\left. F(S)^p = 1 \in \operatorname{Hom}(G_{\mu,1}{}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}}) \right\} / < 1+\mu S > .$$

Therefore by 4.39, 4.15 and (8) we have the thesis. $\square$

Corollary 4.47. *Let us suppose $p > 2$. Let $\mu, \lambda \in R \setminus \{0\}$ be with $v(\lambda_{(1)}) \geq v(\mu) \geq v(\lambda)$. Then, $\{\mathcal{E}^{(\mu,\lambda;F,j)}\}$ is isomorphic to the group*

$$\Phi_{\mu,\lambda} := \Big\{(a,j) \in (R/\lambda R)^{\mathrm{F}} \times \mathbb{Z}/p\mathbb{Z} \text{ such that } pa - j\mu = \frac{p}{\mu^{p-1}} a^p \in R/\lambda^p R\Big\},$$

through the map

$$(a,j) \longmapsto \mathcal{E}^{(\mu,\lambda;\sum_{i=0}^{p-1}\frac{a^i}{i!}S^i,j)}.$$

Remark 4.48. It is clear that if $(0,j) \in \Phi_{\mu,\lambda}$, with $j \neq 0$, then $\mu \equiv 0 \mod \lambda^p$.

Proof. By 4.15, 4.22, (8) and 4.40 (for the case $v(\lambda) = 0$) it follows that $rad_{p,\lambda}(< 1 + \mu S >)$ is isomorphic to

$$\Big\{(a,j) \in (R/\lambda R)^{\mathrm{F}} \times \mathbb{Z}/p\mathbb{Z} | \exists \boldsymbol{b} \in \widehat{W}(R/\lambda^p R)^{\mathrm{F}} \text{ such that } p[a] - j[\mu] = [\frac{p}{\mu^{p-1}}]\boldsymbol{b} + V(\boldsymbol{b}) \in \widehat{W}(R/\lambda^p R)\Big\}. \tag{34}$$

Let a, j and $\boldsymbol{b} = (b_0, b_1, \dots)$ be as above.

By [22, 5.10],

$$p[a] \equiv (pa, a^p, 0, \dots) \mod p^2.$$

Since $[\mu] \in \widehat{W}(R/\lambda^p R)^{\mathrm{F}}$ it follows by 4.9 that

$$j[\mu] = [j\mu] \tag{35}$$

and

$$p[a] - j[\mu] = (pa - j\mu, a^p, 0, 0, \dots, 0, \dots) \in \widehat{W}(R/\lambda^p R). \tag{36}$$

We recall that

$$[\frac{p}{\mu^{p-1}}]\boldsymbol{b} = (\frac{p}{\mu^{p-1}} b_0, \dots, (\frac{p}{\mu^{p-1}})^{p^i} b_i, \dots),$$

then, again by 4.9, we have

$$[\frac{p}{\mu^{p-1}}]\boldsymbol{b} + V(\boldsymbol{b}) = (\frac{p}{\mu^{p-1}} b_0, (\frac{p}{\mu^{p-1}})^p b_1 + b_0, \dots, (\frac{p}{\mu^{p-1}})^{p^{i+1}} b_{i+1} + b_i, \dots). \tag{37}$$

Since $\boldsymbol{b} \in \widehat{W}(R/\lambda^p R)$ there exists $r \geq 0$ such that $b_i = 0$ for any $i \geq r$. Moreover, comparing (36) and (37), it follows

$$(\frac{p}{\mu^{p-1}})^{p^i} b_{i+1} + b_i = 0 \quad \text{for } i \geq 1$$
$$(\frac{p}{\mu^{p-1}})^p b_1 + b_0 = a^p$$
$$(\frac{p}{\mu^{p-1}})^p b_0 = pa - j\mu.$$

So $b_i = 0$ if $i \geq 1$, $b_0 = a^p$ and $pa - j\mu = \frac{p}{\mu^{p-1}} a^p$. □

Example 4.49. Let us suppose $\mu = \lambda = \lambda_{(1)}$. Then $G_{\lambda_{(1)}} \simeq \mathbb{Z}/p\mathbb{Z}$. By 4.36, 4.47 and 4.39 we have that

$$\{(k\eta, k) | k \in \mathbb{Z}/p\mathbb{Z}\} \subseteq \Phi_{\lambda_{(1)},\lambda_{(1)}} \simeq rad_{p,\lambda_{(1)}}(< 1 + \lambda_{(1)} S >).$$

On the other hand by 4.39 and 4.44 it follows that $rad_{p,\lambda_{(1)}}(< 1 + \lambda_{(1)} S >) \simeq H_0^2(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$. Therefore $\{(k\eta, k) | k \in \mathbb{Z}/p\mathbb{Z}\} \simeq rad_{p,\lambda_{(1)}}(< 1 + \lambda_{(1)} S >)$.

We now concentrate on to the case $v(\mu) \geq v(\lambda)$, which is the unique case, as proved in 4.45, where extensions of $G_{\mu,1}$ by $G_{\lambda,1}$ could be models of $\mathbb{Z}/p^2\mathbb{Z}$, as group schemes. Our task is to find explicitly all the solutions $(a,j) \in (R/\lambda R)^{\mathrm{F}}$ of the equation $pa - j\mu = a^p \in R/\lambda^p R$. By 4.47 this means finding explicitly all the extensions of type $\mathcal{E}^{(\mu,\lambda;F,j)}$. Let us consider the restriction map

$$r : \{\mathcal{E}^{(\mu,\lambda;F,j)}\} \longrightarrow \mathrm{Ext}^1_K(\mu_p,\mu_p) \simeq \mathbb{Z}/p\mathbb{Z}.$$

We remark that it coincides with the projection

$$p_2 : \left\{(a,j) \in (R/\lambda R)^{\mathrm{F}} \times \mathbb{Z}/p\mathbb{Z} \text{ such that } pa - j\mu = \frac{p}{\mu^{p-1}} a^p \in R/\lambda^p R\right\} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

So there is an extension of $G_{\mu,1}$ by $G_{\lambda,1}$ which is a model of $(\mathbb{Z}/p^2\mathbb{Z})_K$ if and only if p_2 is surjective. First of all we describe explicitly the kernel of the above map.

Lemma 4.50. *We have*

$$\ker p_2 = \Big\{(a,0) \in R/\lambda R \times \mathbb{Z}/p\mathbb{Z} \textit{ s. t., for any lifting } \tilde{a} \in R,$$
$$pv(\tilde{a}) \geq \max\{pv(\lambda) + (p-1)v(\mu) - v(p), v(\lambda)\}\Big\}$$

In particular p_2 is injective if and only if $v(\lambda) \leq 1$ or $v(p) - (p-1)v(\mu) < p$.

Proof. Let $(a,0) \in \ker p_2 \cap R/\lambda R \times \mathbb{Z}/p\mathbb{Z}$. By the definitions we have that

$$pa = \frac{p}{\mu^{p-1}} a^p \in R/\lambda^p R \quad \text{ and } \quad a^p = 0 \in R/\lambda R.$$

Let $\tilde{a} \in R$ be a lift of a. Since $v(\mu) \geq v(\lambda)$, if $a \neq 0$ then $v(\tilde{a}) < v(\mu)$. Hence

$$v(p) + v(\tilde{a}) > pv(\tilde{a}) + v(p) - (p-1)v(\mu) \tag{38}$$

Therefore

$$pa = \frac{p}{\mu^{p-1}} a^p \in R/\lambda^p R$$

if and only if

$$\frac{p}{\mu^{p-1}} a^p = 0 \in R/\lambda^p R,$$

if and only if

$$pv(\tilde{a}) + v(p) - (p-1)v(\mu) \geq pv(\lambda).$$

We remark that $a^p = 0 \in R/\lambda R$ means $pv(\tilde{a}) \geq v(\lambda)$. So we have proved the first assertion. Now if $v(\lambda) \leq 1$ or $v(p) - (p-1)v(\mu) < p$ it is easy to see that there are no nonzero elements in $\ker p_2$. While if $v(\lambda) > 1$ and $v(p) - (p-1)v(\mu) \geq p$, take $a \in R/\lambda R$ with a lifting $\tilde{a} \in R$ of valuation $v(\lambda) - 1$. Therefore

$$p(v(\lambda) - 1) \geq \max\{pv(\lambda) - v(p) + (p-1)v(\mu), v(\lambda)\}.$$

Hence $(a,0) \in \ker p_2$. □

We remark that $\ker p_2$ depends only on the valuations of μ and λ. So we can easily compute $\Phi_{\mu,\lambda}$, too.

Proposition 4.51. *Let us suppose $p > 2$. Let $\mu, \lambda \in R \setminus \{0\}$ be with $v(\lambda_{(1)}) \geq v(\mu) \geq v(\lambda)$.*

a) *If $v(\mu) < pv(\lambda)$ then p_2 is surjective if and only if $pv(\mu) - v(\lambda) \geq v(p)$. And, if p_2 is surjective, $\Phi_{\mu,\lambda}$ is isomorphic to the group*

$$\{(j\eta\frac{\mu}{\lambda_{(1)}} + \alpha, j) | (\alpha, 0) \in \ker(p_2) \textit{ and } j \in \mathbb{Z}/p\mathbb{Z}\}$$

For the definition of η see 4.36.

b) *If $v(\mu) \geq pv(\lambda)$ then p_2 is surjective and $\Phi_{\mu,\lambda}$ is isomorphic to*
$$\{(\alpha, j) | (\alpha, 0) \in \ker(p_2) \text{ and } j \in \mathbb{Z}/p\mathbb{Z}\} \simeq \ker p_2 \times \mathbb{Z}/p\mathbb{Z}.$$

c) *If p_2 is not surjective then p_2 is the zero morphism. So $\Phi_{\mu,\lambda} = \ker p_2$.*

Remark 4.52. Let us suppose $v(\mu) < pv(\lambda)$. Let $(b, j) \in \Phi_{\mu,\lambda}$ with $j \neq 0$. By 4.48, then $b \neq 0$. Let $\tilde{b} \in R$ be any of its lifting. Then $v(\tilde{b}) = v(\eta\frac{\mu}{\lambda_{(1)}}) = v(\mu) - \frac{v(p)}{p}$. Indeed, by the theorem, we have $\tilde{b} = \eta\frac{\mu}{\lambda_{(1)}} + \alpha$ for some $\alpha \in R/\lambda R$ with $v(\tilde{\alpha}) > v(\eta\frac{\mu}{\lambda_{(1)}}) = v(\mu) - \frac{v(p)}{p}$, where $\tilde{\alpha} \in R$ is any lifting of α.

Proof. a) First, we suppose that p_2 is surjective. This is equivalent to saying that
$$pa - j\mu = \frac{p}{\mu^{p-1}}a^p \in R/\lambda R \tag{39}$$
has a solution $a \in (R/\lambda R)^{\mathrm{F}}$ if $j \neq 0$. Since $v(\mu) < v(p)$, by (38) it follows that
$$v(\mu) = v(p) - (p-1)v(\mu) + pv(\tilde{a}), \tag{40}$$
with $\tilde{a} \in R$ a lifting of a. Since $a \in (R/\lambda R)^{\mathrm{F}}$ we have $pv(\tilde{a}) \geq v(\lambda)$. Hence, by (40), $pv(\mu) - v(\lambda) \geq v(p)$.

Conversely let us suppose that $pv(\mu) - v(\lambda) \geq v(p)$. We know by 4.36 and 4.44 that
$$p\eta - \lambda_{(1)} = \frac{p}{\lambda_{(1)}^{p-1}}\eta^p \in R/\lambda_{(1)}^p R.$$
We recall that $v(\eta) = v(\lambda_{(2)})$. Since $pv(\lambda_{(1)}) - v(\lambda_{(1)}) + \mu \geq p\mu \geq p\lambda$, if we divide the above equation by $\frac{\lambda_{(1)}}{\mu}$ we obtain
$$p\eta\frac{\mu}{\lambda_{(1)}} - \mu = \frac{p}{\mu^{(p-1)}}(\frac{\mu}{\lambda_{(1)}}\eta)^p \in R/\lambda^p R.$$
We remark that $\eta\frac{\mu}{\lambda_{(1)}} \in (R/\lambda R)^{\mathrm{F}}$, since, by hypothesis, $v\big((\eta\frac{\mu}{\lambda_{(1)}})^p\big) = pv(\mu) - v(p) \geq v(\lambda)$. Clearly $j\eta\frac{\mu}{\lambda_{(1)}}$ is a solution of (39) for any $j \in \mathbb{Z}/p\mathbb{Z}$.

In particular it follows that, if p_2 is surjective, $\Phi_{\mu,\lambda}$ is isomorphic to the group
$$\{(j\eta\frac{\mu}{\lambda_{(1)}} + \alpha, j) | (\alpha, 0) \in \ker(p_2) \text{ and } j \in \mathbb{Z}/p\mathbb{Z}\}$$

b) If $v(\mu) \geq pv(\lambda)$ then we have that $\mu = 0 \in R/\lambda^p R$. We remark that $(0, j) \in \Phi_{\mu,\lambda}$. This implies that p_2 is surjective and that $(\alpha, j) \in R/\lambda R \times \mathbb{Z}/p\mathbb{Z} \cap \Phi_{\mu,\lambda}$ if and only if $(\alpha, 0) \in \ker(p_2)$.

c) Since p_2 is a morphism of groups with target $\mathbb{Z}/p\mathbb{Z}$ then the image of p_2 is a subgroup of $\mathbb{Z}/p\mathbb{Z}$. Then the image of p_2 is trivial or it is equal to $\mathbb{Z}/p\mathbb{Z}$. The assertion follows.

□

Example 4.53. Let us suppose $v(\mu) = v(\lambda_{(1)})$, i.e. $G_{\mu,1} \simeq \mathbb{Z}/p\mathbb{Z}$. For simplicity we will suppose $\mu = \lambda_{(1)}$. Then p_2 is an isomorphism. Indeed in this case $\ker(p_2) = 0$ by 4.50 and it is surjective by 4.51(a)-(b). This means that, in this case, any extension $\mathcal{E}^{(\lambda_{(1)},\lambda;F,j)}$ is uniquely determined by the induced extension over K. Let us now consider the map
$$\mathrm{Ext}^1(G_{\lambda_{(1)},1}, G_{\lambda_{(1)},1}) \longrightarrow \mathrm{Ext}^1(G_{\lambda_{(1)},1}, G_{\lambda,1})$$
induced by the map $\mathbb{Z}/p\mathbb{Z} \simeq G_{\lambda_{(1)},1} \longrightarrow G_{\lambda,1}$ given by $S \mapsto \frac{\lambda_{(1)}}{\lambda}S$. It is easy to see that $\mathcal{E}^{(\lambda_{(1)},\lambda;F,j)}$ is the image of $\mathcal{E}^{(\lambda_{(1)},\lambda_{(1)};E_p(\eta S),j)}$ through the above map. Indeed from the above proposition we have that $F(S) \equiv E_p(\eta S) \mod \lambda$. We remark that if $pv(\lambda) \leq v(\lambda_{(1)})$ then $\eta \equiv 0 \mod \lambda$, indeed in such a case $v(\lambda) \leq v(\lambda_{(2)}) = v(\eta)$.

4.9. **Classification of models of** $(\mathbb{Z}/p^2\mathbb{Z})_K$**.** By the previous paragraphs we have a classification of extensions of $G_{\mu,1}$ by $G_{\lambda,1}$ whose generic fibre is isomorphic, as group scheme, to $\mathbb{Z}/p^2\mathbb{Z}$. But this classification is too fine for our tasks. We want here to forget the structure of extension. We are only interested in the group scheme structure. We observe that it can happen that two non isomorphic extensions are isomorphic as group schemes. We here study when it happens.

First of all we recall what the model maps between models of $\mathbb{Z}/p\mathbb{Z}$ are. Let us suppose $\varrho, \tilde{\varrho} \in R$ with $v(\varrho), v(\tilde{\varrho}) \leq v(\lambda_{(1)})$. Since $G_{\varrho,1}$ is flat over R, by 4.13 it follows that the restriction map

$$\mathrm{Hom}_{gr}(G_{\varrho,1}, G_{\tilde{\varrho},1}) \longrightarrow \mathrm{Hom}_{gr}((G_{\varrho,1})_K, (G_{\tilde{\varrho},1})_K) \simeq \mathbb{Z}/p\mathbb{Z}$$

in an injection. It follows easily by (10) that

$$\mathrm{Hom}_{gr}(G_{\varrho,1}, G_{\tilde{\varrho},1}) = \begin{cases} \mathbb{Z}/p\mathbb{Z}, & \text{if } v(\varrho) \geq v(\tilde{\varrho}); \\ 0, & \text{if } v(\varrho) < v(\tilde{\varrho}), \end{cases}$$

where, in the first case, the morphisms are given by $S \longmapsto \frac{(1+\varrho S)^r - 1}{\tilde{\varrho}}$ with $r \in \mathbb{Z}/p\mathbb{Z}$. We remark that, if $v(\varrho) = v(\tilde{\varrho})$ and $r \neq 0$, these morphisms are isomorphisms.

We now recall that by 4.1, 4.44, 4.47 and 4.45 any model of $(\mathbb{Z}/p^2\mathbb{Z})_K$ is of the form $\mathcal{E}^{(\mu,\lambda;F,j)}$ such that $j \neq 0$, $v(\lambda_{(1)}) \geq v(\mu) \geq v(\lambda)$ and $F(S) = \sum_{i=0}^{p-1} \frac{a^i}{i!} S^i$ with $(a, j) \in \Phi_{\mu,\lambda}$. See 4.51 for the explicit description of $\Phi_{\mu,\lambda}$. For $i = 1, 2$ let us consider $\mathcal{E}^{(\mu_i,\lambda_i;F_i,j_i)}$, models of $(\mathbb{Z}/p^2\mathbb{Z})_K$. First of all we remark that there is an injection

$$r_K : \mathrm{Hom}(\mathcal{E}^{(\mu_1,\lambda_1,F_1,j_1)}, \mathcal{E}^{(\mu_2,\lambda_2,F_2,j_2)}) \longrightarrow \mathrm{Hom}_K(\mathcal{E}_{j_1,K}, \mathcal{E}_{j_2,K})$$

given by

$$f \longmapsto (\alpha_{\mu_2,\lambda_2})_K \circ f_K \circ (\alpha_{\mu_1,\lambda_1})_K^{-1}$$

See (33) for the definition $\alpha_{\mu,\lambda}$. We recall that

$$\mathrm{Hom}(\mathcal{E}_{j_1}, \mathcal{E}_{j_2}) \simeq \mathrm{Hom}_K(\mathcal{E}_{j_1,K}, \mathcal{E}_{j_2,K}).$$

and the elements are the morphisms

$$\psi_{r,s} : \mathcal{E}_{j_1} \longrightarrow \mathcal{E}_{j_2},$$

which, on the level of Hopf algebras, are given by

$$S_1 \longmapsto S_1^{\frac{rj_1}{j_2}} \tag{41}$$

$$S_2 \longmapsto S_1^s S_2^r, \tag{42}$$

for some $r \in \mathbb{Z}/p\mathbb{Z}$ and $s \in \mathbb{Z}/p\mathbb{Z}$. Moreover the map

$$\begin{aligned} \mathrm{Hom}(\mathcal{E}_{j_1}, \mathcal{E}_{j_2}) &\longrightarrow \mathbb{Z}/p^2\mathbb{Z} \\ \psi_{r,s} &\longmapsto r + \frac{p}{j_1} s \end{aligned}$$

is an isomorphism. So $\mathrm{Hom}(\mathcal{E}^{(\mu_1,\lambda_1,F_1,j_1)}, \mathcal{E}^{(\mu_2,\lambda_2,F_2,j_2)})$ is a subgroup of $\mathbb{Z}/p^2\mathbb{Z}$ through the map r_K. We remark that the unique nontrivial subgroup of $\mathrm{Hom}(\mathcal{E}_{j_1}, \mathcal{E}_{j_2})$ is $\{\psi_{0,s} | s \in \mathbb{Z}/p\mathbb{Z}\}$. Finally we have that any morphism $\mathcal{E}^{(\mu_1,\lambda_1,F_1,j_1)} \longrightarrow \mathcal{E}^{(\mu_2,\lambda_2,F_2,j_2)})$ is given by

$$\begin{aligned} S_1 &\longrightarrow \frac{(1+\mu_1 S_1)^{\frac{rj_1}{j_2}} - 1}{\mu_2} \\ S_2 &\longrightarrow \frac{(F_1(S_1) + \lambda_1 S_2)^r (1+\mu_1 S_1)^s - F_2(\frac{(1+\mu_1 S_1)^{\frac{rj_1}{j_2}} - 1}{\mu_2})}{\lambda_2}, \end{aligned} \tag{43}$$

for some $r, s \in \mathbb{Z}/p\mathbb{Z}$. With abuse of notation we call it $\psi_{r,s}$. We remark that the morphisms $\psi_{r,s} : \mathcal{E}^{(\mu_1,\lambda_1,F_1,j_1)} \longrightarrow \mathcal{E}^{(\mu_2,\lambda_2,F_2,j_2)}$ which are model maps correspond, by (41), to $r \neq 0$. In

such a case $\psi_{r,s}$ is a morphism of extensions, i.e. there exist morphisms $\psi_1 : G_{\lambda,1} \longrightarrow G_{\lambda,2}$ and $\psi_2 : G_{\mu,1} \longrightarrow G_{\mu,2}$ such that

$$\begin{tikzcd} 0 \arrow[r] & G_{\lambda_1,1} \arrow[r] \arrow[d, "\psi_1"] & \mathcal{E}^{(\mu_1,\lambda_1,F_1,j_1)} \arrow[r] \arrow[d, "\psi_{r,s}"] & G_{\mu_1,1} \arrow[r] \arrow[d, "\psi_2"] & 0 \\ 0 \arrow[r] & G_{\lambda_2,1} \arrow[r] & \mathcal{E}^{(\mu_2,\lambda_2,F_2,j_2)} \arrow[r] & G_{\mu_2,1} \arrow[r] & 0 \end{tikzcd} \tag{44}$$

commutes. More precisely ψ_1 is given by $S \mapsto \frac{(1+\lambda_1 S)^r - 1}{\lambda_2}$ and ψ_2 by $S \mapsto \frac{(1+\mu S_1)^{\frac{rj_1}{j_2}} - 1}{\mu_2}$.

We now calculate $\mathrm{Hom}(\mathcal{E}^{(\mu_1,\lambda_1,F_1,j_1)}, \mathcal{E}^{(\mu_2,\lambda_2,F_2,j_2)})$.

Proposition 4.54. *For $i = 1,2$, if $F_i(S) = E_p(a_i S) = \sum_{k=0}^{p-1} \frac{a_i^k}{k!} S^i$ and $\mathscr{E}_i = \mathcal{E}^{(\mu_i,\lambda_i;F_i,j_i)}$ are models of $(\mathbb{Z}/p^2\mathbb{Z})_K$ we have*

$$\mathrm{Hom}(\mathscr{E}_1, \mathscr{E}_2) = \begin{cases} 0, & \text{if } v(\mu_1) < v(\lambda_2); \\ \{\psi_{r,s}\} \simeq \mathbb{Z}/p^2\mathbb{Z}, & \text{if } v(\mu_2) \le v(\mu_1),\ v(\lambda_2) \le v(\lambda_1) \\ & \text{and } a_1 \equiv \frac{j_1}{j_2}\frac{\mu_1}{\mu_2} a_2 \mod \lambda_2; \\ \{\psi_{0,s}\} \simeq \mathbb{Z}/p\mathbb{Z}, & \text{otherwise.} \end{cases}$$

Proof. It is immediate to see that $\psi_{0,s} \in \mathrm{Hom}(\mathscr{E}_1, \mathscr{E}_2)$, with $s \neq 0$, if and only if $v(\mu_1) \ge v(\lambda_2)$. We now see conditions for the existence of $\psi_{r,s}$ with $r \neq 0$. If it exists, in particular, we have two morphisms $G_{\mu_1,1} \longrightarrow G_{\mu_2,1}$ and $G_{\lambda_1,1} \longrightarrow G_{\lambda_2,1}$. This implies $v(\mu_1) \ge v(\mu_2)$ and $v(\lambda_1) \ge v(\lambda_2)$. Moreover we have that

$$F_1(S_1)^r (1+\mu_1 S_1)^s = F_2\left(\frac{(1+\mu_1 S_1)^{\frac{rj_1}{j_2}} - 1}{\mu_2}\right) \in \mathrm{Hom}(G_{\mu_1,1|S_{\lambda_2}}, \mathbb{G}_{m|S_{\lambda_2}}).$$

Since $v(\mu_1) \ge v(\mu_2) \ge v(\lambda_2)$, we have

$$F_1(S_1)^r = F_2\left(\frac{(1+\mu_1 S_1)^{\frac{rj_1}{j_2}} - 1}{\mu_2}\right) \in \mathrm{Hom}(G_{\mu_1,1|S_{\lambda_2}}, \mathbb{G}_{m|S_{\lambda_2}}). \tag{45}$$

If we define the morphism of groups

$$\begin{aligned} [\frac{\mu_1}{\mu_2}]^* : \mathrm{Hom}(G_{\mu_2,1|S_{\lambda_2}}, \mathbb{G}_{m|S_{\lambda_2}}) &\longrightarrow \mathrm{Hom}(G_{\mu_1,1|S_{\lambda_2}}, \mathbb{G}_{m|S_{\lambda_2}}) \\ F(S_1) &\longmapsto F(\frac{\mu_1}{\mu_2} S_1) \end{aligned}$$

then

$$\begin{aligned} F_2\left(\frac{(1+\mu_1 S_1)^{\frac{rj_1}{j_2}} - 1}{\mu_2}\right) &= [\frac{\mu_1}{\mu_2}]^* \left(F_2 \left(\frac{(1+\mu_1 S_1)^{\frac{rj_1}{j_2}} - 1}{\mu_1} \right) \right) \\ &= [\frac{\mu_1}{\mu_2}]^* (F_2(S_1))^{\frac{rj_1}{j_2}} \\ &= F_2(\frac{\mu_1}{\mu_2}(S_1))^{\frac{rj_1}{j_2}}. \end{aligned}$$

Therefore we have

$$F_1(S_1)^r = (F_2(\frac{\mu_1}{\mu_2} S_1))^{\frac{rj_1}{j_2}} \in \mathrm{Hom}(G_{\mu_1,1|S_{\lambda_2}}, \mathbb{G}_{m|S_{\lambda_2}}). \tag{46}$$

Every element of $\mathrm{Hom}(G_{\mu_1,1|S_\lambda}, \mathbb{G}_{m|S_\lambda})$ has order p. Let t be an inverse for r modulo p. Then raising the equality to the t^{th}-power we obtain

$$F_1(S_1) = (F_2(\frac{\mu_1}{\mu_2} S_1))^{\frac{j_1}{j_2}} \in \mathrm{Hom}(G_{\mu_1,1|S_{\lambda_2}}, \mathbb{G}_{m|S_{\lambda_2}}).$$

By 4.22 this means

$$a_1 \equiv \frac{j_1}{j_2}\frac{\mu_1}{\mu_2}a_2 \mod \lambda_2.$$

It is conversely clear that, if $v(\mu_1) \geq v(\mu_2)$, $v(\lambda_1) \geq v(\lambda_2)$ and

$$F_1(S_1) = (F_2(\frac{\mu_1}{\mu_2}S_1))^{\frac{j_1}{j_2}} \in \mathrm{Hom}(G_{\mu_1,1|S_{\lambda_2}}, \mathbb{G}_{m|S_{\lambda_2}}),$$

then (43) defines a morphism of group schemes.

□

We have the following result which gives a criterion to determine the class of isomorphism, as a group scheme, of an extension of type $\mathcal{E}^{(\mu,\lambda;F,j)}$.

Corollary 4.55. *For $i = 1, 2$, let $F_i(S) = E_p(aS) = \sum_{k=0}^{p-1} \frac{a_i^k}{k!}S^k$ and let $\mathscr{E}_i = \mathcal{E}^{(\mu_i,\lambda_i;F_i,j_i)}$ be models of $(\mathbb{Z}/p^2\mathbb{Z})_K$. Then they are isomorphic if and only if $v(\mu_1) = v(\mu_2)$, $v(\lambda_1) = v(\lambda_2)$ and $a_1 \equiv \frac{j_1}{j_2}\frac{\mu_1}{\mu_2}a_2 \mod \lambda_2$. Moreover if it happens then any model map between them is an isomorphism.*

Proof. By the proposition we have that a model map $\psi_{r,s} : \mathcal{E}^{(\mu_1,\lambda_1,F_1,j_1)} \longrightarrow \mathcal{E}^{(\mu_2,\lambda_2,F_2,j_2)}$ exists if and only if $v(\mu_1) \geq v(\mu_2)$, $v(\lambda_1) \geq v(\lambda_2)$ and $a_1 \equiv \frac{j_1}{j_2}\frac{\mu_1}{\mu_2}a_2 \mod \lambda_2$. It is a morphism of extensions as remarked before the proposition. Let us consider the commutative diagram (41). Then $\psi_{r,s}$ is an isomorphism if and only if ψ_i is an isomorphism for $i = 1, 2$. By the discussion made at the beginning of this section this is equivalent to requiring $v(\mu_1) = v(\mu_2)$ and $v(\lambda_1) = v(\lambda_2)$. This also proves the last assertion. □

We remarked that if $v(\mu_1) = v(\mu_2)$ and $v(\lambda_1) = v(\lambda_2)$ then

$$\mathrm{Ext}^1(G_{\mu_1,1}, G_{\lambda_1,1}) \simeq \mathrm{Ext}^1(G_{\mu_2,1}, G_{\lambda_2,1}).$$

The following is a more precise statement for extensions of type $\mathcal{E}^{(\mu,\lambda;F,j)}$.

Corollary 4.56. *Let $\mathcal{E}^{(\mu_1,\lambda_1;E_p(aS),j)} \in \mathrm{Ext}^1(G_{\mu_1,1}, G_{\lambda_1,1})$ be a model of $\mathbb{Z}/p^2\mathbb{Z}$. Then for any μ_2, λ_2 such that $v(\mu_1) = v(\mu_2)$ and $v(\lambda_1) = v(\lambda_2)$ we have*

$$\mathcal{E}^{(\mu_1,\lambda_1;E_p(aS),j)} \simeq \mathcal{E}^{(\mu_2,\lambda_2;E_p(\frac{a}{j}\frac{\mu_2}{\mu_1}S),1)}$$

as group schemes.

Proof. Firstly we prove that there exists the group scheme $\mathcal{E}^{(\mu_2,\lambda_2;E_p(\frac{a}{j}\frac{\mu_2}{\mu_1}S),1)}$. By 4.47 we have that $a \in (R/\lambda R)^{\mathrm{F}}$ and

$$pa - j\mu_1 = \frac{p}{\mu_1^{p-1}}a^p \mod \lambda_1^p. \tag{47}$$

Then, multiplying (47) by $\frac{\mu_2}{\mu_1}\frac{1}{j}$, we have

$$p\frac{a\mu_2}{j\mu_1} - \mu_2 \equiv \frac{p}{\mu_2^{p-1}}\left(\frac{a\mu_2}{j\mu_1}\right)^p \mod \lambda_2^p.$$

Hence $\mathcal{E}^{(\mu_2,\lambda_2;E_p(\frac{a}{j}\frac{\mu_2}{\mu_1}S),1)}$ is a group scheme (see again 4.47). Then by the above proposition we can conclude that

$$\mathcal{E}^{(\mu_1,\lambda_1;E_p(aS),j)} \simeq \mathcal{E}^{(\mu_2,\lambda_2;E_p(\frac{a}{j}\frac{\mu_2}{\mu_1}S),1)}$$

as group schemes.

□

Example 4.57. Let $\mu, \lambda \in R$ be such that $v(\mu) = v(\lambda) = v(\lambda_{(1)})$. We now want to describe $\mathbb{Z}/p^2\mathbb{Z}$ as $\mathcal{E}^{(\mu,\lambda;F,1)}$. We recall that we defined

$$\eta = \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \lambda_{(2)}^k$$

By 4.36 and the previous corollary we have

$$\mathbb{Z}/p^2\mathbb{Z} \simeq \mathcal{E}^{(\mu,\lambda;E_p(\eta\frac{\mu}{\lambda_{(1)}}S),1)}.$$

We conclude the section with the complete classification of $(\mathbb{Z}/p^2\mathbb{Z})_K$-models. The following theorem summarizes the above results.

Theorem 4.58. *Let us suppose $p > 2$. Let G be a finite and flat R-group scheme such that $G_K \simeq (\mathbb{Z}/p^2\mathbb{Z})_K$. Then $G \simeq \mathcal{E}^{(\pi^m,\pi^n;E_p(aS),1)}$ for some $v(\lambda_{(1)}) \geq m \geq n \geq 0$ and $(a, 1) \in \Phi_{\pi^m,\pi^n}$. Moreover m, n and $a \in R/\pi^n R$ are unique.*

Remark 4.59. The explicit description of the set Φ_{π^m,π^n} has been given in 4.51 and 4.50.

Proof. By 4.1, 4.44, 4.45, 4.47 and 4.56 any model of $(\mathbb{Z}/p^2\mathbb{Z})_K$ is of type $\mathcal{E}^{(\pi^m,\pi^n;E_p(aS),1)}$ with $m \geq n$ and $(a, 1) \in \Phi_{\pi^m,\pi^n}$. By 4.55, it follows that,

$$\mathcal{E}^{(\pi^{m_1},\pi^{n_1},E_p(a_1S),1)} \simeq \mathcal{E}^{(\pi^{m_2},\pi^{n_2},E_p(a_2S),1)}$$

as group schemes if and only if $m_1 = m_2$, $n_1 = n_2$ and $a_1 = a_2 \in R/\pi^{n_1}R$. □

5. Reduction on the special fiber of the models of $(\mathbb{Z}/p^2\mathbb{Z})_K$

In the following we study the special fibers of the extensions of type $\mathcal{E}^{(\lambda,\mu,;F,j)}$ with $v(\mu) \geq v(\lambda)$. In particular, by 4.45, this includes the extensions which are models of $(\mathbb{Z}/p^2\mathbb{Z})_K$ as group schemes. We study separately the different cases which can occur.

5.1. **Case $\mathbf{v}(\mu) = \mathbf{v}(\lambda) = \mathbf{0}$.** We have $(G_{\lambda,1})_k \simeq (G_{\mu,1})_k \simeq \mu_p$. The extensions of type $\mathcal{E}^{(\lambda,\mu,;F,j)}$ are the extensions $\mathcal{E}_i$ with $i \in \mathbb{Z}/p\mathbb{Z}$. The special fibers of the extensions $\mathcal{E}_i$ with $i \in \mathbb{Z}/p\mathbb{Z}$ are clearly $\mathcal{E}_{i,k}$. See also 4.33.

5.2. **Case $\mathbf{v}(\lambda_{(1)}) \geq \mathbf{v}(\mu) > \mathbf{v}(\lambda) = \mathbf{0}$.** In such a case we have $(G_{\lambda,1})_k \simeq \mu_p$. It is immediate by the definitions that any extension $\mathcal{E}^{(\mu,\lambda;1,j)}$ is trivial on the special fiber.

5.3. **Case $\mathbf{v}(\lambda_{(1)}) > \mathbf{v}(\mu) \geq \mathbf{v}(\lambda) > \mathbf{0}$.** Then $(G_{\mu,1})_k \simeq (G_{\lambda,1})_k \simeq \alpha_{p,k}$.

First, we recall some results about extensions of group schemes of order p over a field k. See [4, III §6 7.7.] for a reference.

Theorem 5.1. *Let us suppose that α_p acts trivially on α_p over k. The exact sequence*

$$0 \longrightarrow \alpha_p \to \mathbb{G}_a \xrightarrow{\mathrm{F}} \mathbb{G}_a \to 0$$

induces the following split exact sequence

$$0 \longrightarrow \mathrm{Hom}_k(\alpha_p, \mathbb{G}_a) \longrightarrow \mathrm{Ext}^1(\alpha_p, \alpha_p) \longrightarrow \mathrm{Ext}^1(\alpha_p, \mathbb{G}_a) \longrightarrow 0.$$

It is also known that

$$\mathrm{Ext}^1(\mathbb{G}_a, \mathbb{G}_a) \simeq H_0^2(\mathbb{G}_a, \mathbb{G}_a) \longrightarrow H_0^2(\alpha_p, \mathbb{G}_a) \simeq \mathrm{Ext}^1(\alpha_p, \mathbb{G}_a).$$

is surjective. Since $\mathrm{Ext}^1(\mathbb{G}_a, \mathbb{G}_a) \simeq H_0^2(\mathbb{G}_a, \mathbb{G}_a)$ is freely generated as a right $k[\mathrm{F}]$-module by $C_i = \frac{X^{p^i}+X^{p^i}-(X+Y)^{p^i}}{p^i}$ and $D_i = XY^{p^i}$ for all $i \in \mathbb{N} \setminus \{0\}$, it follows that $H_0^2(\alpha_p, \mathbb{G}_a) \simeq \mathrm{Ext}^1(\alpha_p, \mathbb{G}_a)$ is freely generated as right k-module by the class of the cocycle $C_1 = \frac{X^p+X^p-(X+Y)^p}{p}$. So $\mathrm{Ext}^1(\alpha_p, \mathbb{G}_a) \simeq k$.

Moreover it is easy to see that $\mathrm{Hom}_k(\alpha_p, \mathbb{G}_a) \simeq k$. The morphisms are given by $T \mapsto aT$ with $a \in k$. By these remarks we have that the isomorphism

$$\mathrm{Hom}_k(\alpha_p, \mathbb{G}_a) \times \mathrm{Ext}^1(\alpha_p, \mathbb{G}_a) \longrightarrow \mathrm{Ext}^1(\alpha_p, \alpha_p),$$

deduced from 5.1, is given by

$$(\beta, \gamma C_1) \mapsto E_{\beta,\gamma}.$$

The extension $E_{\beta,\gamma}$ is so defined:

$$E_{\beta,\gamma} = \mathrm{Spec}(k[S_1, S_2]/(S_1^p, S_2^p - \beta S_1))$$

(1) law of multiplication

$$\begin{aligned} S_1 &\longmapsto S_1 \otimes 1 + 1 \otimes S_1 \\ S_2 &\longmapsto S_2 \otimes 1 + 1 \otimes S_2 + \gamma \frac{S_1^p \otimes 1 + 1 \otimes S_1^p - (S_1 \otimes 1 + 1 \otimes S_1)^p}{p} \end{aligned}$$

(2) unit

$$\begin{aligned} S_1 &\longmapsto 0 \\ S_2 &\longmapsto 0 \end{aligned}$$

(3) inverse

$$\begin{aligned} S_1 &\longmapsto -S_1 \\ S_2 &\longmapsto -S_2 \end{aligned}$$

It is clear that all such extensions are commutative. In [22, 4.3.1] the following result was proved.

Proposition 5.2. *Let $\lambda, \mu \in \pi R \setminus \{0\}$. Then $[\mathcal{E}_k^{(\mu,\lambda;E_p(\boldsymbol{a},\mu,S))}] \in H_0^2(\mathbb{G}_{a,k}, \mathbb{G}_{a,k})$ coincides with the class of*

$$\sum_{k=1}^{\infty} \frac{(\mathrm{F} - [\mu^{p-1}])(\tilde{\boldsymbol{a}})}{\lambda} C_k,$$

where $\tilde{\boldsymbol{a}} \in \widehat{W}(R)$ is a lifting of $\boldsymbol{a} \in \widehat{W}(R/\lambda R)$.

We deduce the following corollary about the extensions of α_p by $\mathbb{G}_a$.

Corollary 5.3. *Let $\lambda, \mu \in \pi R \setminus \{0\}$. Then $[\tilde{\mathcal{E}}_k^{(\mu,\lambda;E_p(\boldsymbol{a},\mu,S))}] \in H_0^2(\alpha_{p,k}, \mathbb{G}_{a,k})$ coincides with the class of*

$$\frac{(\mathrm{F} - [\mu^{p-1}])(\tilde{\boldsymbol{a}})}{\lambda} C_1,$$

where $\tilde{\boldsymbol{a}} \in \widehat{W}(R)$ is a lifting of $\boldsymbol{a} \in \widehat{W}(R/\lambda R)$.

Proof. This follows from the fact that $\mathcal{E}_k^{(\mu,\lambda;E_p(\boldsymbol{a},\mu,S))} \mapsto \tilde{\mathcal{E}}_k^{(\mu,\lambda;E_p(\boldsymbol{a},\mu,S))}$ through the map

$$\mathrm{Ext}^1(\mathbb{G}_a, \mathbb{G}_a) \simeq H_0^2(\mathbb{G}_a, \mathbb{G}_a) \longrightarrow H_0^2(\alpha_p, \mathbb{G}_a) \simeq \mathrm{Ext}^1(\alpha_p, \mathbb{G}_a).$$

□

Let us take an extension $\mathcal{E}^{(\mu,\lambda;E_p(aS),j)}$. Let $\tilde{a}$ be a lifting of a. We have that on the special fiber this extension is given as a scheme by

$$\mathcal{E}_k^{(\mu,\lambda;E_p(aS),j)} = \mathrm{Spec}(k[S_1, S_2]/(S_1^p, S_2^p - (-\frac{(\sum_{i=0}^{p-1} \frac{\tilde{a}^i}{i!} S^i)^p (1 + \mu S_1)^{-j} - 1}{\lambda^p}))).$$

By 4.47 we know that

$$pa - j\mu - \frac{p}{\mu^{p-1}} a^p = 0 \in R/\lambda^p R$$

In the proof of the same corollary we have seen that

$$p[a] - j[\mu] - [\frac{p}{\mu^{p-1}} a^p] - V([a^p]) = [pa - j\mu - \frac{p}{\mu^{p-1}} a^p] \in \widehat{W}(R/\lambda^p R).$$

By the definitions we have the following equality in $\mathrm{Hom}(\mathcal{G}^{(\mu)}_{|S_{\lambda^p}}, \mathbb{G}_{m|S_{\lambda^p}})$

$$\xi^0_{R/\lambda^p R}(p[a]-j[\mu]-[\frac{p}{\mu^{p-1}}a^p]-V([a^p])) = E_p(aS_1)^p(1+\mu S_1)^{-j}\left(E_p\left(a^p\left(\frac{(1+\mu S_1)^p-1}{\mu}\right)\right)\right)^{-1}.$$

Moreover we have

$$\xi^0_{R/\lambda^p R}([pa-j\mu-\frac{p}{\mu^{p-1}}a^p]) = E_p((pa-j\mu-\frac{p}{\mu^{p-1}}a^p)S_1)$$

So we have that

$$\begin{aligned}(\sum_{i=0}^{p-1}\frac{\tilde a^i}{i!}S_1^i)^p(1+\mu S_1)^{-j}-1 &\equiv \sum_{i=0}^{p-1}\frac{(pa-j\mu-\frac{p}{\mu^{p-1}}a^p)^i S_1^i}{i!}-1\\ &\equiv 0 \mod \lambda^p\left(R[S_1]/(\frac{(1+\lambda S_1)^p-1}{\lambda^p})\right).\end{aligned}$$

Hence

$$\begin{aligned}\frac{(\sum_{i=0}^{p-1}\frac{\tilde a^i}{i!}S_1^i)^p(1+\mu S_1)^{-j}-1}{\lambda^p} &\equiv \frac{\sum_{i=0}^{p-1}\frac{(pa-j\mu-\frac{p}{\mu^{p-1}}a^p)^i}{i!}S_1^i-1}{\lambda^p}\\ &\equiv \frac{(pa-j\mu-\frac{p}{\mu^{p-1}}a^p)}{\lambda^p}S_1 \mod \pi.\end{aligned}$$

On the other hand $\mathcal{E}_k^{(\mu,\lambda;E_p(aS),j)} \mapsto \tilde{\mathcal{E}}_k^{(\mu,\lambda;E_p(aS))}$ through the map $\mathrm{Ext}^1(\alpha_p,\alpha_p)\to\mathrm{Ext}^1(\alpha_p,\mathbb{G}_a)$.

Therefore $\mathcal{E}_k^{(\mu,\lambda;E_p(aS),j)} \simeq E_{\beta,\gamma}$ with $\beta = (-\frac{p\tilde a-j\mu-\frac{p}{\mu^{p-1}}\tilde a^p}{\lambda^p} \mod \pi)$ and $\gamma = (\frac{\tilde a^p}{\lambda} \mod \pi)$. We have so proved the following result.

Proposition 5.4. *Let $\lambda,\mu\in\pi R$ be such that $v(\lambda)\le v(\mu)<v(\lambda_{(1)})$. Then $[\mathcal{E}_k^{(\mu,\lambda;E_p(aS),j)}]\in \mathrm{Ext}^1_k(\alpha_p,\alpha_p)$ coincides with the class of*

$$\left(-\frac{p\tilde a-j\mu-\frac{p}{\mu^{p-1}}\tilde a^p}{\lambda^p}, \frac{\tilde a^p}{\lambda}C_1\right),$$

where $\tilde a\in R$ is a lifting of $a\in R/\lambda R$.

5.4. **Case $\mathbf{v}(\lambda_{(1)})=\mathbf{v}(\mu)>\mathbf{v}(\lambda)>0$.** In this situation we have

$$(G_{\mu,1})_k\simeq \mathbb{Z}/p\mathbb{Z} \quad\text{ and }\quad (G_{\lambda,1})_k\simeq\alpha_p.$$

Proposition 5.5. *Let $\lambda,\mu\in\pi R$ be such that $v(\mu)=v(\lambda_{(1)})>v(\lambda)$. Then $\mathcal{E}_k^{(\mu,\lambda;E_p(aS),j)}$ is the trivial extension.*

Proof. We can suppose $\mu=\lambda_{(1)}$. From 4.53 it follows that $\mathcal{E}^{(\lambda_{(1)},\lambda;F,j)}$ is in the image of the morphism

$$\mathrm{Ext}^1(G_{\lambda_{(1)},1},G_{\lambda_{(1)},1})\longrightarrow \mathrm{Ext}^1(G_{\lambda_{(1)},1},G_{\lambda,1})$$

induced by the map $\mathbb{Z}/p\mathbb{Z}\simeq G_{\lambda_{(1)},1}\longrightarrow G_{\lambda,1}$ given by $S\mapsto\frac{\lambda_{(1)}}{\lambda}S$. But this morphism is the zero morphism on the special fiber. So we are done. □

5.5. **Case $\mathbf{v}(\lambda_{(1)})=\mathbf{v}(\mu)=\mathbf{v}(\lambda)$.** We have

$$(G_{\mu,1})_k\simeq\mathbb{Z}/p\mathbb{Z} \quad\text{ and } (G_{\lambda,1})_k\simeq\mathbb{Z}/p\mathbb{Z}.$$

For simplicity we will suppose $\mu=\lambda=\lambda_{(1)}$. We recall the following result.

Proposition 5.6. *Let suppose that $\mathbb{Z}/p\mathbb{Z}$ acts trivially on $\mathbb{Z}/p\mathbb{Z}$ over k. The exact sequence $0\to\mathbb{Z}/p\mathbb{Z}\to\mathbb{G}_a\stackrel{\mathrm{F}-1}{\to}\mathbb{G}_a\to 0$ induces the following exact sequence*

$$\begin{aligned}\mathrm{Hom}_{gr}(\mathbb{Z}/p\mathbb{Z},\mathbb{G}_a)\simeq k\xrightarrow{\mathrm{F}-1}\mathrm{Hom}_{gr}(\mathbb{Z}/p\mathbb{Z},\mathbb{G}_a)\simeq k\longrightarrow \mathrm{Ext}^1_k(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}/p\mathbb{Z})\longrightarrow\\ \longrightarrow\mathrm{Ext}^1_k(\mathbb{Z}/p\mathbb{Z},\mathbb{G}_a)\simeq k\xrightarrow{\mathrm{F}-1}\mathrm{Ext}^1_k(\mathbb{Z}/p\mathbb{Z},\mathbb{G}_a)\simeq k\end{aligned}$$

Proof. [4] $\square$

We observe that $\ker\left(\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z},\mathbb{G}_a)\xrightarrow{\mathrm{F}-1}\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z},\mathbb{G}_a)\right)\simeq\mathbb{Z}/p\mathbb{Z}$. It is possible to describe more explicitly $\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}/p\mathbb{Z})$. We recall that $\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z},\mathbb{G}_a)=H^2_0(\mathbb{Z}/p\mathbb{Z},\mathbb{G}_a)$ is freely generated as a right k-module by the class of the cocycle $C_1=\frac{X^p+X^p-(X+Y)^p}{p}$.

There is an isomorphism, induced by the maps of 5.6,

$$k/(\mathrm{F}-1)(k)\times\mathbb{Z}/p\mathbb{Z}\longrightarrow\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}/p\mathbb{Z}),$$

given by

$$(a,b)\mapsto E_{a,b}.$$

The extension $E_{a,b}$ is so defined: let $\bar{a}\in k$ a lifting of a,

$$E_{a,b}=\mathrm{Spec}(k[S_1,S_2]/(S_1^p-S_1,S_2^p-S_2-\bar{a}S_1))$$

(1) law of multiplication

$$S_1\longmapsto S_1\otimes1+1\otimes S_1$$
$$S_2\longmapsto S_2\otimes1+1\otimes S_2+b\frac{S_1^p\otimes1+1\otimes S_1^p-(S_1\otimes1+1\otimes S_1)^p}{p}$$

(2) unit

$$S_1\longmapsto 0$$
$$S_2\longmapsto 0$$

(3) inverse

$$S_1\longmapsto -S_1$$
$$S_2\longmapsto -S_2$$

We remark that the extensions which are isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ as group schemes are the extensions $E_{0,b}$ with $b\neq0$. By 4.49 we have that any extension of $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$ is given by $\mathcal{E}^{(\lambda_{(1)},\lambda_{(1)};E_p(j\eta S),j)}$. We now study its reduction on the special fiber.

Proposition 5.7. *For any $j\in\mathbb{Z}/p\mathbb{Z}$, $[\mathcal{E}_k^{(\lambda_{(1)},\lambda_{(1)};E_p(j\eta S),j)}]=E_{0,j}\in\mathrm{Ext}^1_k(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}/p\mathbb{Z})$.*

Proof. As group schemes, $\mathcal{E}^{(\lambda_{(1)},\lambda_{(1)};E_p(j\eta S),j)}\simeq\mathbb{Z}/p^2\mathbb{Z}$, if $j\neq0$, and $\mathcal{E}^{(\lambda_{(1)},\lambda_{(1)};1,0)}\simeq\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ otherwise. In particular $\mathcal{E}_k^{(\lambda_{(1)},\lambda_{(1)};E_p(j\eta S),j)}$ has a scheme-theoretic section. It is easy to see that $\mathcal{E}_k^{(\lambda_{(1)},\lambda_{(1)};E_p(j\eta S),j)}\simeq E_{0,b}$ with

$$b=(-j\frac{\eta^p}{\lambda_{(1)}(p-1)!}\mod\pi)=j,$$

since $\frac{\eta^p}{\lambda_{(1)}}\equiv\frac{\lambda_{(2)}^p}{\lambda_{(1)}}\equiv1\mod\pi$ and $(p-1)!\equiv-1\mod\pi$ (Wilson Theorem). $\square$

References

[1] F. Andreatta et C. Gasbarri – "Torsors under some group schemes of order p^n", *J. Algebra* **318** (2007), no. 2, p. 1057–1067.

[2] M. F. Atiyah et I. G. Macdonald – *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[3] S. Bosch, W. Lütkebohmert et M. Raynaud – *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

[4] M. Demazure et P. Gabriel – *Groupes algebrique*, vol. I, North-Holland Publishing company, 1970.

[5] B. Green et M. Matignon – "Liftings of Galois covers of smooth curves", *Compositio Math.* **113** (1998), no. 3, p. 237–272.

[6] C. Greither – "Extensions of finite group schemes, and hopf galois theory over a complete discrete valuation ring", *Mathematische Zeitschrift* (1992), no. 210, p. 37–67.

[7] Q. Liu – *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, 2002.

[8] J. S. Milne – *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

[9] F. Oort et J. Tate – "Group schemes of prime order", *Ann. Sci. École Norm. Sup. (4)* **3** (1970), p. 1–21.

[10] M. Raynaud – "Schémas en groupes de type $(p, \dots, p)$", *Bull. Soc. Math. France* **102** (1974), p. 241–280.

[11] L. G. Roberts – "The flat cohomology of group schemes of rank p", *American Journal of Mathematics* **95** (1973), no. 3, p. 688–702.

[12] M. Romagny – "Sur quelques aspects des champs de revêtements de courbes algébriques", Thèse, Institut Fourier, Univ. Grenoble 1, 2002.

[13] T. Sekiguchi – "On the unification of Kummer and Artin-Schreier-Witt theories", *Sūrikaisekikenkyūsho Kōkyūroku* (2001), no. 1200, p. 1–12, Algebraic number theory and related topics (Japanese) (Kyoto, 2000).

[14] T. Sekiguchi, F. Oort et N. Suwa – "On the deformation of Artin-Schreier to Kummer", *Ann. Sci. École Norm. Sup. (4)* **22** (1989), no. 3, p. 345–375.

[15] T. Sekiguchi et N. Suwa – "Some cases of extensions of group schemes over a discrete valuation ring. II", *Bull. Fac. Sci. Engrg. Chuo Univ. Ser. I Math.* **32** (1989), p. 17–35.

[16] ———, "A case of extensions of group schemes over a discrete valuation ring", *Tsukuba J. Math.* **14** (1990), no. 2, p. 459–487.

[17] ———, "On the deformations of Witt groups to tori II", *J. Algebra* **138** (1991), p. 273–297.

[18] ———, "Some cases of extensions of group schemes over a discrete valuation ring. I", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **38** (1991), no. 1, p. 1–45.

[19] ———, "Théories de Kummer-Artin-Schreier-Witt", *C. R. Acad. Sci. Paris Sér. I Math.* **319** (1994), no. 2, p. 105–110.

[20] ———, "Théorie de Kummer-Artin-Schreier et applications", *J. Théor. Nombres Bordeaux* **7** (1995), no. 1, p. 177–189.

[21] ———, "On the unified Kummer-Artin-Schreier-Witt theory", *Mathématiques Pures de Bordeaux C.N.R.S* (1999), Prepublication.

[22] ———, "A note on extensions of algebraic and formal groups. IV. Kummer-Artin-Schreier-Witt theory of degree p^2", *Tohoku Math. J. (2)* **53** (2001), no. 2, p. 203–240.

[23] ———, "A note on extensions of algebraic and formal groups. V", *Japan. J. Math. (N.S.)* **29** (2003), no. 2, p. 221–284.

[24] D. Tossici – "Effective models and extension of torsors over a d.v.r. of unequal characteristic", 2008, arXiv:math/0803.3730v1.

[25] W. C. Waterhouse – "Principal homogeneous spaces and group scheme extensions", *Transactions of the American Mathematical Society* **153** (1971), p. 181–189.

[26] ———, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979.

[27] ———, "A unified Kummer-Artin-Schreier sequence", *Math. Ann.* **277** (1987), no. 3.

[28] W. C. Waterhouse et B. Weisfeiler – "One-dimensional affine group schemes", *J. Algebra* **66** (1980), no. 2, p. 550–568.

Dipartimento di Matematica, Università di Roma Tre, Rome, Italy
E-mail address: dajano@mat.uniroma3.it